https://www.pwc.co.nz/services/pwc-legal.html

Artificial intelligence: What directors need to know

Trusted AI
Accelerate responsibly

December 2023

pwc

The era of AI has well and truly begun...

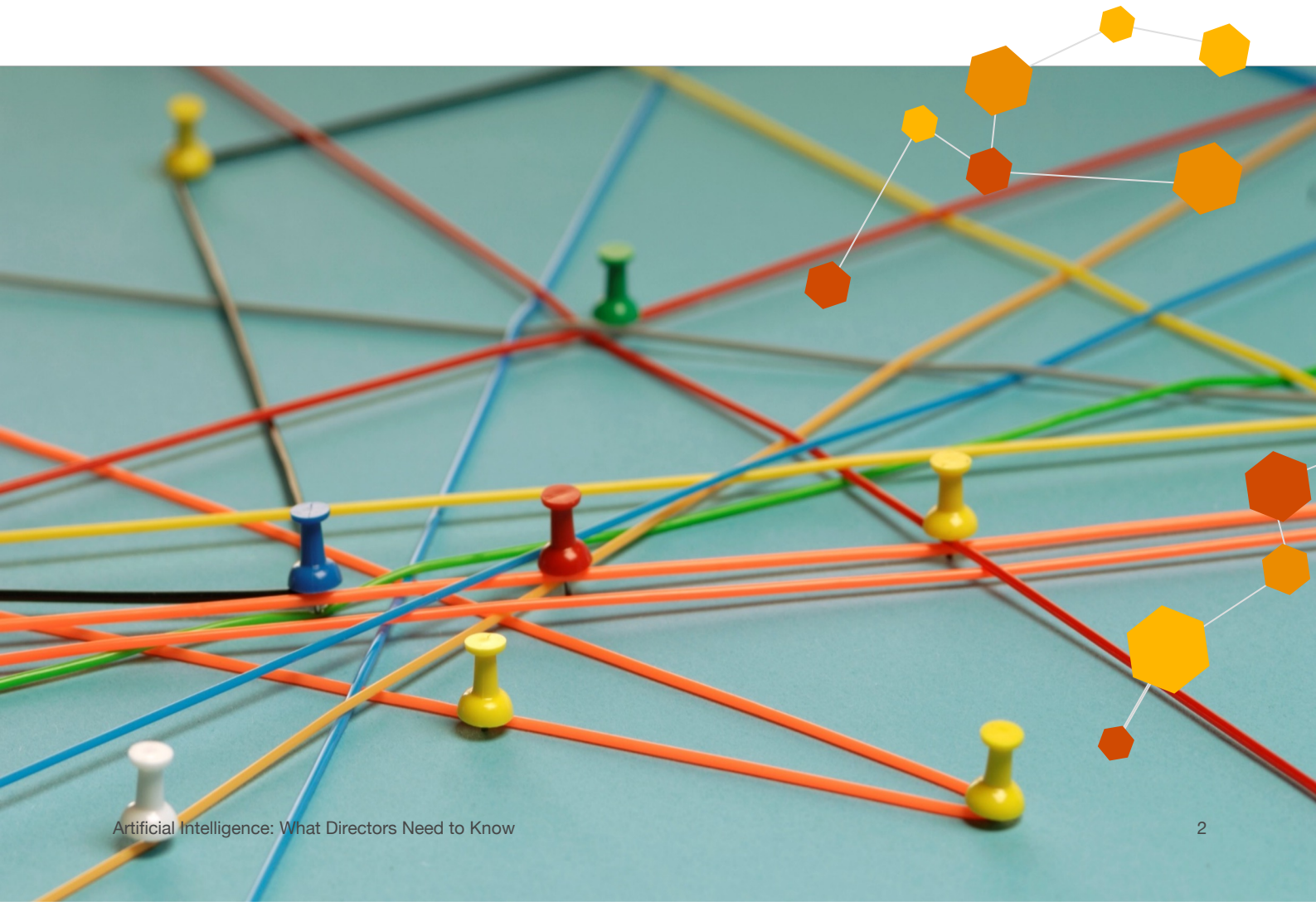
With generative artificial intelligence (AI) tools like ChatGPT well and truly becoming an 'overnight' sensation, many have been awakened to the potential for AI to revolutionise the way we do business. But the reality is that the use of AI technologies in everyday business functions is already commonplace. From Netflix using AI to recommend movies based on what we have previously watched, to the agricultural industry using AI for crop and soil management or e-commerce product recommendation engines re-targeting consumers based on past purchases, AI is already disrupting traditional business.

In light of the staggering increase in AI use, directors are under mounting pressure to ensure their organisations are prepared to use AI in a responsible manner. But what does this really mean in practice?

New Zealand laws have yet to clearly define what AI is, let alone what a director's duties are when it comes to AI. Although specific black letter law regulating AI has yet to be formalised, directors need to understand their role and responsibilities in the deployment of AI. In short, that means implementing AI governance.

AI is happening *now*, and directors should look to stay ahead of the curve. The choice is not between using AI and not using AI. Given its prevalence and trajectory, AI will either be used by an organisation governed or ungoverned – the choice is in the hands of the directors.

This article looks to unpack the relevance of directors' duties in the context of AI and how directors can effectively manage these duties. AI, with all its promises and opportunities, comes with a range of known risks. Without appropriate organisational governance, there is a real possibility that AI becomes a source of harm and risk (and therefore, liability) to your business.



Key takeaways

Given the increasing trend of using AI in the workplace, understanding the technology and its impact within the organisation and the boardroom falls directly within the scope of a director's obligation to act in good faith and in the best interests of the company when discharging his or her duties.

Accordingly, directors must:

Examine legal and regulatory consequences

Despite a lack of explicit AI laws in New Zealand, legal obligations may arise from existing governing legislative instruments or regulations e.g. privacy, human rights, or anti-discrimination laws. Directors should be aware of how the use of AI in their organisations may contravene these laws, and ensure mitigating processes are put in place to manage compliance.

Implement appropriate AI governance

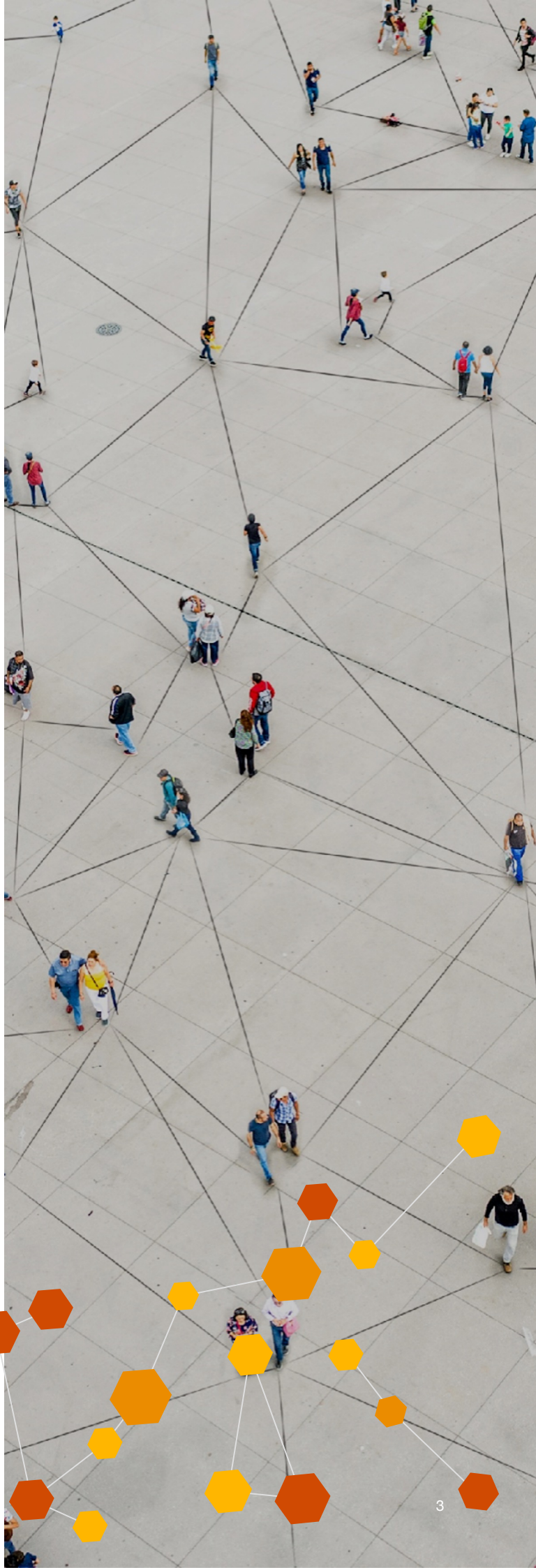
Directors must turn their minds to AI because it affects every aspect of their oversight duties. Directors and officers must consider how to manage the data, models and people involved in implementing AI. Critically, directors cannot determine risk effectively for their organisation in the modern world without dealing with the impact of AI.

Consider the risks of AI use

Directors must consider the impact of the use of AI on society, people and organisations. Risks to an organisation can be commercial, regulatory and reputational in nature. In particular, consider the impact on your organisation's key stakeholders such as your employees and customers. Consider also the risks of not adopting AI solutions.

Ensure ongoing assurance of AI

Like any other business risk, AI is not a 'set and forget' obligation – routine assurance of AI systems, and the governance framework itself, is required to ensure compliance with regulations and best practice.



How do director duties extend to AI?

Under the Companies Act 1993 (the Companies Act), directors have a duty to:

- act in good faith and in the best interests of the company (which may be evaluated, at the directors' discretion, by consideration of matters other than the maximisation of profit such as environmental, social and governance matters);[1] and
- exercise the care, diligence, and skill that a reasonable director would exercise in the same circumstances, considering the nature of the company, the nature of the decision and the position of the director and the nature of responsibilities undertaken.[2]

While there is no exhaustive statutory checklist of matters for directors to follow in determining what is in the best interests of the company, the Courts have accepted that directors, acting properly, are best-equipped to use their discretion to determine the best interests of the company.

This typically requires directors to implement good governance procedures in order to act in good faith to promote the benefit of the company. In this regard, it is important that directors understand the risks posed by AI (discussed further on page 5), and the characteristics of good governance (discussed further on page 13).

The broad reference to discretionary consideration of environment, social or governance (ESG) factors when assessing whether an action is in the best interests of a company is a recent amendment to the Companies Act. In contrast, directors in the United Kingdom have been required to have regard for ESG factors since 2006.

As to how AI fits within the ESG agenda, the United Kingdom's Institute of Directors (UK IOD) Science, Innovation and Technology Expert Advisory Group has published guidance for boards. It notes that AI should be included on the board agenda and "considered seriously as part of the G in ESG and the CSR (Corporate Social Responsibility) requirements".[3] The paper sets out 12 principles for boards to consider, summarised as follows:

- monitor the evolving regulatory environment
- continually audit and measure what AI is in use
- undertake impact assessments which consider the business and wider stakeholder community
- establish board accountability
- set high level goals for AI in the business aligned with its values
- empowering a diverse, cross functional ethics committee that has the power to veto
- document and secure data sources
- train people to get the best out of AI and to interpret the results
- comply with privacy by design requirements
- comply with 'secure by design' requirements
- test and remove from use if bias and other impacts are discovered; and
- review regularly.

Similarly, the New Zealand Institute of Directors (NZ IOD) has noted the need to monitor legislative and regulatory developments in relation to AI, potentially re-evaluate intellectual property (IP) strategies and assess ethical and social implications advising that directors and boards should engage in discussions about these issues and consider how their organisations' policies and practices align with broader societal values.[4]

In order for directors to fulfil their duties to a company, they are required to make decisions involving discrete and finely balanced judgment. AI may not always be able to pick up on subtle changes in stakeholder interests in the same way humans can. AI can also be guilty of generating false information (e.g, hallucinations, as discussed on page 7). Directors should keep such limitations in mind when considering the use of, and reliance on, AI within their organisation.

Can directors be held liable for improper use of AI in a company or AI 'gone wrong'?

The short answer is yes.

Directors may be personally exposed to legal liability if they fail to uphold their statutory duties, including to act in good faith and with care, diligence and skill, when overseeing the use of AI in their organisation. Ultimately, they will remain liable for any final decision-making, despite using AI tools to reach each decision.

In certain cases, the consequences of directors breaching their duties can be significant and directors should be aware that their liability is not precluded by the limited liability company structure. At a personal level, directors may:

- in extreme cases face criminal sanctions, including in some cases imprisonment;
- face civil proceedings culminating in potentially substantial pecuniary penalties and/or compensation awards, and legal costs;
- be disqualified from being a director or taking part in the management of a company; or
- lose professional standing and reputation.

1 *Companies Act 1993*, s 131.
2 *Companies Act 1993*, s 137.
3 https://www.iod.com/resources/blog/science-innovation-and-tech/ai-in-the-boardroom-the-essential-questions-for-your-next-board-meetin/
4 https://www.iod.org.nz/news/articles/the-governance-implications-of-ai-inventorship-lessons-from-the-dabus-case

The risks of AI

The exponential growth in the accessibility to, and capability of AI solutions presents profound opportunities and risks for organisations, people and society at large.

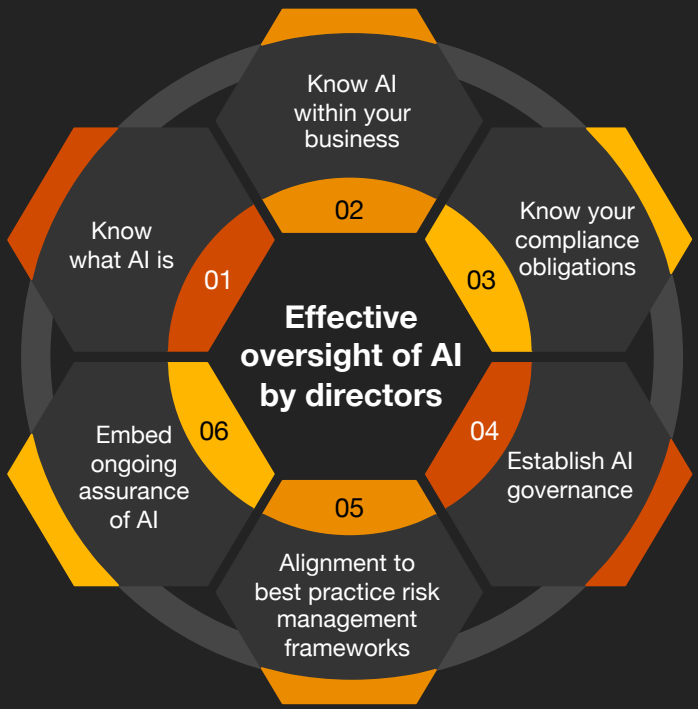
With each new opportunity that AI unlocks, it also brings about a new breed of issues and challenges from operational risk management, ethics and morality and legal standpoints. For example:

- Creating and using AI and related technology can present unique IP issues regarding ownership of AI, IP protection through copyright and other IP regimes, and infringement of such IP.
- Risk of non-compliance with data protection and privacy regulation (e.g. unlawful use of personal information or failure to secure that personal information if cyber security controls in the AI tool are not effective). This risk is heightened due to the size and complexity of utilised data sets.
- Unlawful discrimination or harmful biases caused by imbalances in training data and/or incomplete review of model outputs. Algorithmic bias in AI used for decision-making (e.g. hiring decisions) could lead to a potential breach of anti-discrimination laws, including under the Human Rights Act 1993. This could entrench structural inequalities and disadvantages.
- Reputational damage by failing to meet community expectations around the use of AI in products/ services, and by failing to be transparent about the use of AI.
- While the benefits of AI from a commercial perspective are clear, its use in setting prices and responding to market changes raises potential antitrust risks, in addition to lending itself to potential unlawful, anticompetitive agreements in its operation and use.
- Operational disruptions due to insufficient planning for continuity and resilience for business critical applications of AI.
- Malicious use of AI leading to cyber attacks, fraud and circumvention of security controls.
- Over-reliance on AI for automation (e.g. applying the wrong types of models to use cases, or inadequate human review and output verification).
- Failure to respond to advancements in AI, exposing the organisation to business model disruption.
- Misinformed decisions or inaccurate insights due to quality issues with training data, model design or improper application/usage of a model.
- Use of AI applications developed overseas and trained on international data may not be fit for purpose in New Zealand, based on our demographics.

So, now what?

Appropriate AI governance can, if done correctly, accelerate the growth of a company's uptake and ability to benefit from AI solutions, and ensure directors and officers meet their obligations under the Companies Act.

Set out below is a *list of key activities* that directors should consider for them to be able to effectively oversee the implementation of a good AI corporate governance framework within their company. This doesn't require organisations to reinvent the wheel, in fact, many organisations have existing governance and risk management processes and procedures that can be leveraged to effectively govern AI within the organisation. The trick is identifying those most relevant and augmenting them as required to address the uniqueness of AI solutions.



Key activities directors should consider to effectively implement and oversee governance of AI

1 Know what AI is

AI is a difficult concept to define. Directors need to consider what the company considers to be “AI” for the purposes of its AI governance and establishing appropriate guidelines for AI. Even subtle variances in definition can have major impacts on its application in the organisation. For example; your definition could go as broad as all automated decision systems, or it could be narrowed down to focus on a field of AI (e.g. unsupervised deep learning) or a type of AI (e.g. Generative AI). As a result, it is critical to ensure a functional definition of “AI” is established that reflects the scope that is to be governed.

Some commonly used definitions of AI include:

NZ Government: ‘Artificial Intelligence’ is the field of computer science that seeks to create engineered systems that can generate outputs for particular sets of objectives, without explicit programming.[5]

EU AI Act – ‘Artificial intelligence system’ (AI system) means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate output such as predictions, recommendations, or decisions influencing physical or virtual environments.[6]

While directors are not necessarily expected to become digitally-literate in the sense that they must learn how to code or create AI models themselves, there is a duty for a director in the current day and age to be properly advised on data and technology. Failure to understand their company's use of AI technologies could give rise to a risk of breach of their duties as a company director.

5 ‘Initial advice on Generative Artificial Intelligence in the public service’, issued by Department of Internal Affairs, National Cyber Security Centre, Stats NZ, July 2023.
6 The EU Artificial Intelligence Act, The EU Artificial Intelligence Act (Web Page, 14 June 2023) <https://www.artificial-intelligence-act.com/>.

2 Know AI within your business

Hand in hand with the need to come to a consensus on the definition of AI is the need to understand how AI operates, or is going to operate, in the business.

Directors need to understand the specific type of AI technology captured within the parameters of the business in order to effectively establish a structure which governs and mitigates risks relating to AI. Different AI technologies and their applications will present differing risks that require tailored strategies to mitigate - for instance, Large Language Models (LLMs) hallucinate, posing risks in resiliency and explainability, while autonomous decision-making AI functionalities may pose risks in safety, transparency and accountability. Mitigating these risks requires understanding their interaction with the business' use case and applying relevant controls and monitoring.

Machine Learning Systems – A complex set of machine learning models that collects and uses existing data to develop outputs on new data.

Generative AI – System that generates various types of content, including text, imagery, audio and synthetic data in response to prompts (e.g ChatGPT).

Expert Systems – A computer-based decision-making system that is capable of solving complex problems in specific domains/areas of expertise. Expert systems can advise, diagnose, instruct and assist humans in decision-making, predict results, interpret input, suggest alternatives, amongst other capabilities.

Natural Language Systems – Systems that are able to undertake natural language processing (NLP). Organisations use NLP to read text, hear speech (voice to text), interpret and analyse language-based data, measure sentiment, and determine which parts are important.

Automated Decision-making Systems – Systems that are capable of making a decision by an automated means and without human involvement. The systems can process and analyse large-scale data from various sources to make the decision. It is becoming widely used in public administration e.g. by governments, in business, health, education, law and other sectors, with varying degrees of human intervention or oversight.

FRT (Facial Recognition Technologies) – Any system or device that is capable of determining whether an image contains a face. Often FRT uses biometric data to verify someone's identity, to identify an individual or to analyse characteristics about a person.

Virtual Agents and Chatbots – Chatbots are rule-based software that has been designed to understand and respond to select human keywords or phrases. Virtual agents advance the chatbot functionality – using AI, including natural language processing, to recognise human speech.

Recommendation Systems – Systems that suggest products, services, information to users based on analysis of data, patterns and trends.

AI-powered Robotics – 'Robots' or physical systems that are equipped with various sensors e.g. proximity, computer vision to move and execute tasks in dynamic environments.[10]

A director should look to understand at a high level:

- **AI Technology/Model** – What is the underlying AI technology and how does it work?
- **AI Use Case Benefits** – What is AI being used for within the business? What are the benefits to the organisation through the use of AI? Could these benefits be realised without the use of AI?
- **AI Use Case Risks** – What are the key risks to the organisation through the use of AI? What data is being used to train (or retrain) the AI model? What data is provided to the model for inferencing or prompting purposes? Are compensating controls required to achieve the level of precision that the use case requires?
- **Likelihood of impacts to individuals and groups** – What is the output of the AI model and its level of precision? What are the downstream impacts if AI goes wrong for stakeholders and society more generally?

3 Know your compliance obligations

With AI developing so rapidly, it is no surprise that specific black letter law regulating AI is still playing 'catch-up'. However, in recognition of AI becoming critical to many organisations' operations, governments all around the world are moving swiftly to adapt to the emergence of new AI capabilities.

Some examples include:

- The European Union lawmakers have passed a draft of the Artificial Intelligence Act which is the world's first set of wide-ranging laws related to AI regulation (set out on page 12).[7]
- At the end of March, the UK Government published a white paper setting out how it proposes to approach AI regulation.[8]
- The Australian Government has started a public consultation on how AI should be regulated.[9]

Depending on the geographical footprint of their company, directors will need to be sensitive to the regulatory landscape surrounding AI globally. Directors should consider undertaking a regulatory scan to determine applicable laws and how they might impact on the company's use of AI.

New Zealand has made no specific legislation that deals with AI. The only AI-specific policy is the Algorithm Charter, which largely relates to the public sector and the use of algorithms in public services. Whilst we don't have any AI-specific laws, AI is covered, in part, by existing laws including the Privacy Act, the Human Rights Act, the Companies Act and the Fair Trading Act among others.

There are a number of existing compliance obligations which directors will need to address. These fall under the following headings:

- Privacy & cyber security
- Discrimination in recruitment
- Intellectual property
- Employee relations and health and safety considerations
- Consumer protection
- Competition considerations
- Duty of care and negligence

Privacy and cyber security

There is a slew of privacy issues raised by the use of AI, due to the fact that many AI tools ingest personal information about individuals. Organisations must consider how they will meet the principles of transparency and 'explainability' (the ability to explain how AI uses personal information and comes to a specific output). They must also consider how they will address individual rights requests (the right to access and request correction of information) in relation to data held, or produced by, AI toolsets.

Concerns in relation to fairness are often raised under the umbrella of privacy; this will particularly be the case where an individual does not know that their personal information is being ingested by an AI tool, where they perceive the AI toolset to be overly intrusive or where they feel that the output is inaccurate, biased or otherwise unfair.

Unrestrained by law or ethical concerns, cyber criminals are using AI to develop new innovative ways to exploit and attack technology systems. Directors must therefore ensure appropriate implementation, and ongoing monitoring of cyber security measures in their business, where large data sets are being utilised to train AI models.

Discrimination in recruitment

AI-enhanced HR practices that assist organisations to make hiring decisions may expose an employer to a risk of unintentional discriminatory practices.

It is becoming more widely understood that AI is a potential vehicle for increased risk of employee discrimination due to biases in the input data. Directors must ensure there are safeguards in place in their business to mitigate any instances of discriminatory practices built into and/or resulting from AI and other similar systems.

On the flip side, there may be cases of positive discrimination and inherent bias in input data sets used to train AI algorithms for organisations that are trying to enhance diversity and inclusion in their workplace. Those who claim AI removes all aspects of human biases on gender and ethnicity during recruitment are toeing a fine line. The reality is that AI tools are a technology 'black box' and it may be difficult to ensure fairness and accountability in using these models to make company decisions.

Directors should be mindful that regulation of using automated decision-making tools is likely on its way. In recognition of these emerging technologies in employment practices, New York City passed the Automated Employment Decision Tool law, which makes it unlawful for employers to use automated decision-making tools to screen individuals for employment decisions unless certain parameters and risk mitigation measures are undertaken, e.g. bias audits, data disclosure, and appropriate notification. It will be important for directors in New Zealand to monitor regulatory developments in this space.

7 European Parliament, *'Press room'*, AI Act: a step closer to the first rules on Artificial Intelligence Act (Web Page, 11 May 2023) <https://artificialintelligenceact.eu/>.
8 Gov.uk, *AI regulation: a pro-innovation approach* (Web Page, 29 March 2023) <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach>.
9 https://consult.industry.gov.au/supporting-responsible-ai

Intellectual Property (IP)

The complexities surrounding AI and IP are innumerable, from both a data input and output standpoint. The law in this area is unsettled and it is important for directors to keep up to date with developments. Key issues include:

Do AI-generated works qualify for IP protection, and if so, who owns those IP rights? This differs depending on the type of IP and country.

For example, New Zealand copyright law does allow for AI-generated works to qualify for copyright protection, with the author (and default copyright owner) being the person by whom the arrangements necessary for the creation of the work are undertaken. However, the rights holder will likely need to show active involvement by a human in generating the work (through, for example, conscious input as prompts) to establish authorship.

Some other countries (including Australia and the USA) do not currently allow copyright to exist in AI-generated work. This could lead to issues for businesses trying to enforce AI-generated copyright in these countries.

New Zealand's copyright legislation is currently under review. Points being considered include whether the provisions are appropriate as they relate to AI generated works.

As for patents, in *Thaler v Commissioner of Patents,*[10] the High Court concluded that an 'inventor' could only be a natural person, but did not address whether the creator of, or person instructing, AI that generates an invention could be the 'inventor'. Similar decisions have issued overseas. This means that it is not settled whether AI inventions can be patented.

Given the uncertainty, directors should ensure sufficient policies and procedures are in place to ensure AI is used in an appropriate way in the business, and that accurate records are kept, including on the involvement and creative control exercised by team members when using these tools. Contractual arrangements with AI tool providers should be checked to ensure IP ownership provisions are appropriate. Businesses should also exercise caution if using AI to develop or enhance core assets of the business that the business will want to claim IP rights in. For example, if you are a software product company, consider refraining from use of AI tools to generate the code of your core products.

Using AI tools may make your IP vulnerable to being shared with / leveraged by third parties. Keeping IP assets confidential provides an additional layer of protection. For example, software code can be protected as both a copyright work and as confidential information - if the code is confidential, the risk of someone copying the code is (obviously) reduced. If the code is scraped by or fed into an AI tool, there is a risk that the code could be shared with others.

To mitigate this risk, directors should put procedures in place to ensure that AI tools used by the business have appropriate security controls and that the contractual terms governing use of these tools provide appropriate protection for data inputs. Policies and team training are also useful to mitigate the risk of key assets being unwittingly shared.

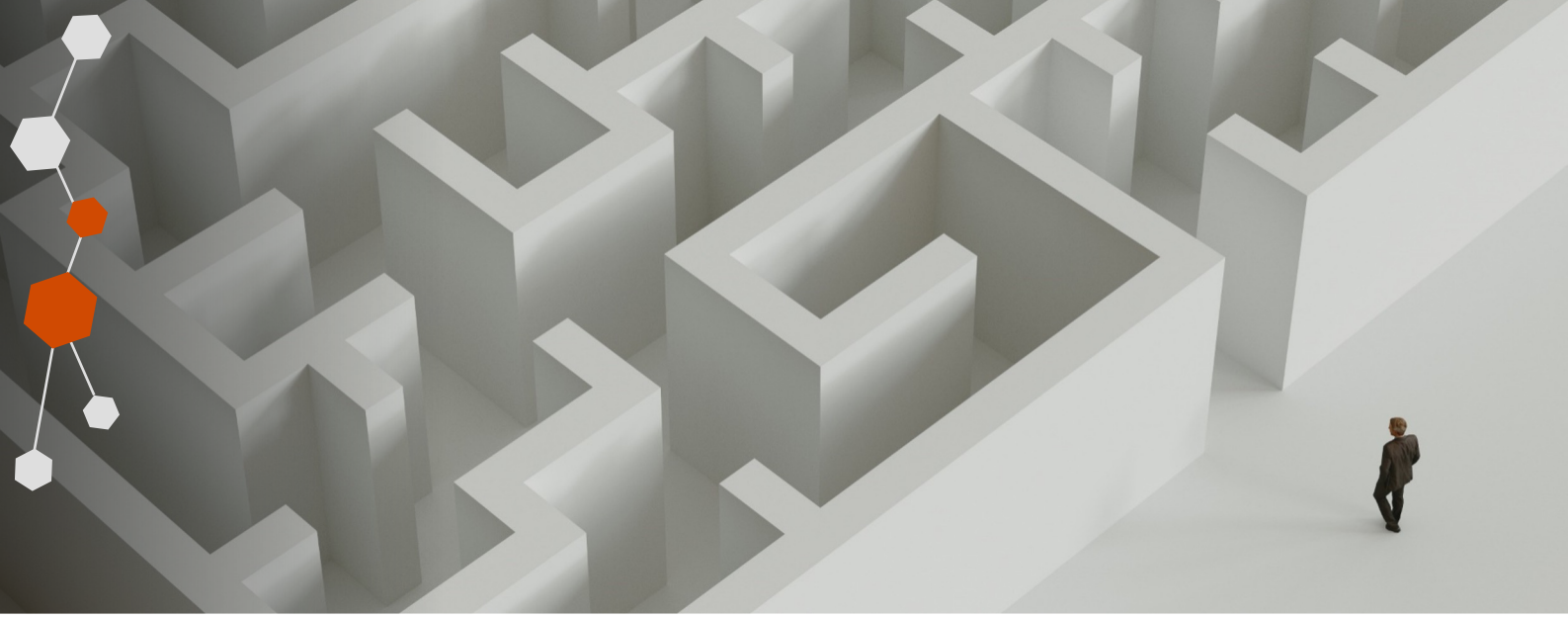
The risk of infringement of third party IP and opensource rights. This will depend on what authorisations were given in relation to the content input into or used by the AI, and whether the AI-generated content is sufficiently different to the original content to avoid infringement. There are a number of cases before the courts internationally considering these issues.

What does this mean for use of AI?

Obviously there are great benefits from using these tools, but there are also some risk points and therefore caution / being deliberate as to what you use it for is key. We suggest being mindful about:

- what generated content is used - for example, if the generated content clearly appears to have been lifted from somewhere else (e.g. for code, due to domain specific information or if it still has comments attached to it), we would advise against using that content
- how AI generated content is used - if the generated content is intended to be used for something critical to the business or something that will be difficult to change in the future, we recommend exercising greater caution in using that content
- what content is input into AI tools - we would not recommend inputting a business' most valuable / unique content (or only inputting content in small chunks) unless there is comfort around the security of the content
- checking contractual arrangements with the AI tool providers to ensure appropriate IP ownership, liability and security arrangements are in place.

10 *Thaler v Commissioner of Patents* [2023] NZHC 554.



Employee relations and health and safety considerations

From an operational perspective, directors must consider the potential detrimental effects of using AI on their workforce.

The introduction of AI is likely to result in organisational structure / role changes in many organisations, as resourcing requirements and company strategies need to be adapted to the impacts of technological changes. In the New Zealand context, employers are required to consult with employees before a decision is made which could impact their ongoing employment. Accordingly, when considering the introduction of AI, and the potential impacts on the workforce shape/size, consultation obligations (in particular, the timing of consultation) should be factored in to mitigate downstream legal risk.

"People problems" arguably require "people solutions" – using technology to monitor and assess employees productivity (e.g. by way of using data to assess or predict employees' talents and capabilities, work outputs, judge states of being and emotions or looking for patterns across workforces of, for example, tendency to use leave or become sick, or probability of resignation) and subsequently make decisions about their performance/progression will potentially expose the organisation's people to heightened structural, physical, and psychosocial risks and stress, which could in turn lead to disputes and legal risk.

While additional monitoring and data will be a useful tool for employers, it will be critical to continue to manage people as people, rather than data points, to meet statutory good faith obligations and ensure a positive employee experience. This includes ensuring that there is meaningful and constructive engagement, and sharing of relevant information to support any concerns.

As organisations and directors have legal obligations to mitigate risks to health and safety in the workplace, the potential for increased prevalence, and new forms of, psychological / wellbeing risks (e.g. increased isolation) is another important factor to be considered.

Consumer protection

The use of AI in the delivery of products or services to consumers will undoubtedly increase the market asymmetry and power dynamic between consumers and businesses.

Whilst our current New Zealand consumer laws were not designed with AI in mind, they certainly will apply to any businesses looking to deploy or promote AI-enabled products or services.

Directors will need to ensure that their organisations consider how AI impacts on compliance with consumer law obligations - this is particularly important as previously flagged, individual directors may be held personally liable for breaches under the Fair Trading Act 1986 (FTA).

For example:

- The FTA prohibits businesses from making unsubstantiated representations in trade. Although AI can be difficult to fully understand (a 'black box', so to speak), any company promoting AI, or products and services which utilise AI, must not make false or overreaching claims about the capability, accuracy, or functionality of a product or service.
- It is unlawful under the FTA to engage in deceptive or misleading conduct in trade. Businesses relying on AI functionality must ensure they truly understand the model and include guardrails regarding truthfulness of outputs. Otherwise, they may be in breach of the FTA, even if the actions were unintentional.
- Use of AI systems in trade or commerce must not result in unconscionable conduct. The fairness of AI in its decision-making is a highly debated topic, and for good reason given the risk of bias. Directors should take care to ensure AI does not breach the FTA in this regard.
- A person involved in trade or commerce must not make false or misleading representations about goods or services or engage in misleading conduct in respect of these goods and services. Any comparisons involving AI products vs other AI products or even non-AI products must be valid, reasonable, accurate and fair.

The reality is that consumer law is designed to protect the 'weaker' party in transactions, and it is only a matter of time before regulators look to insert guardrails to add to protection for consumers against the dangers associated with the use of AI. Directors should monitor this space closely to ensure their company implements processes to ensure compliance with the consumer law at all times with regards to AI.

Competition considerations

It is undeniable that AI technology fundamentally changes the way companies and their directors make decisions, especially in terms of predictive analytics and the optimisation of the decision-making process. AI's ability to trawl through copious amounts of data, compare and extract information at rapid speeds and analyse consumer behaviour to target marketing activities arguably creates many challenges for the existing competition regulations. AI can facilitate collusion, lead to abuse of a dominant position, and reduce competitive pressure, which will affect competition in the market and raise new antitrust considerations. Further, the control and access to data for LLM training and the ownership of AI models also raises competition concerns. Directors must be careful when considering the use of AI in their organisation, especially decisions that impact on the market or go to exclusivity of the provision of AI solutions, so that they do not act in contravention of competition laws.

Duty of care and negligence

General principles of negligence could also apply in the case where AI has caused harm where a duty of care exists. For example, AI might be used by healthcare providers to support the work of human specialists through image analysis. In healthcare, it is accepted that a duty of care exists between a patient and a medical practitioner. Significant reputational consequences could occur if the use of AI misdiagnoses the patient, which then results in significant harm or injury to the person.

To minimise the chance of failing to assert proper care, directors should look to establish processes to sufficiently develop, test, monitor, and supervise any AI system. Any use of AI should be subject to a rigorous risk assessment to identify and mitigate foreseeable harms.

Think about insurance – Whilst not strictly a compliance obligation, company directors should consider the impacts of AI on their existing insurance arrangements. It is possible that insurance policies do not appropriately cover an organisation's use of AI and therefore may not protect the company against certain events that you would ordinarily expect to be covered.

The EU AI Act: a blueprint for AI regulation?

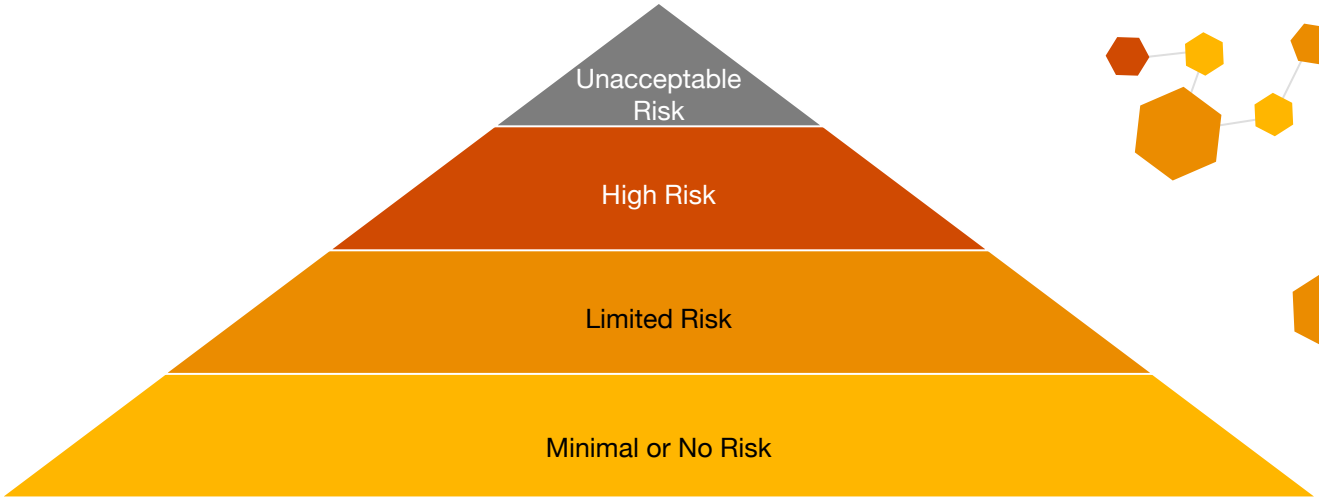
The EU Artificial Intelligence (AI) Act

- If passed into law, the EU AI Act will mark a huge milestone in AI regulation – it will be the world's first legislation that looks to regulate the development and use of AI generally.
- These changes are designed to ensure that AI systems will function with appropriate human oversight and transparency relative to their 'risk' profile.

Key takeaways:

- The EU AI Act is intended to have an extraterritorial impact on the development and use of AI both within EU and overseas. It intends to regulate AI systems which are developed, used and sold within the EU, as well as AI systems that are used outside the EU but produce outputs that are used in the EU. For example, the EU General Data Protection Regulations, if your organisation is or is going to use AI in the EU, this legislation must be considered.
- The EU AI Act sets out a risk-based classification system that assigns a risk rating to the proposed AI technology – each risk rating has associated regulatory obligations.
- The AI Act proposes four risk tiers: Unacceptable, High, Limited and Minimal.
  - AI systems that pose *Unacceptable Risk* are prohibited in the EU, with little exception.
  - Those that pose *High Risk* are subject to substantive and strict obligations under the AI Act.
  - AI systems that pose *Limited Risk* are subject to transparency and notification obligations.
  - AI systems that pose *Minimal or No Risk* can be used in the EU with no restrictions.
- There are enforceable undertakings linked to the AI Act, including significant penalties for breach and non-compliance with the AI Act.

As New Zealand continues its discussions on AI regulation, organisations must remain aware that there are developments occurring in other jurisdictions e.g. the EU, that may also impact on its business.



4 Establish a good AI governance framework

In order to use AI tools responsibly, there is a need to establish a robust, holistic, and accessible governance framework that underpins the development, implementation, procurement and use of AI technologies. Directors may be held personally liable for acts or omissions that could breach their duty to act in good faith or duty of care to the Company. It is not difficult to see how this could be applied in an AI context. As a result, directors should look to oversee that an appropriate AI governance framework is developed and implemented.

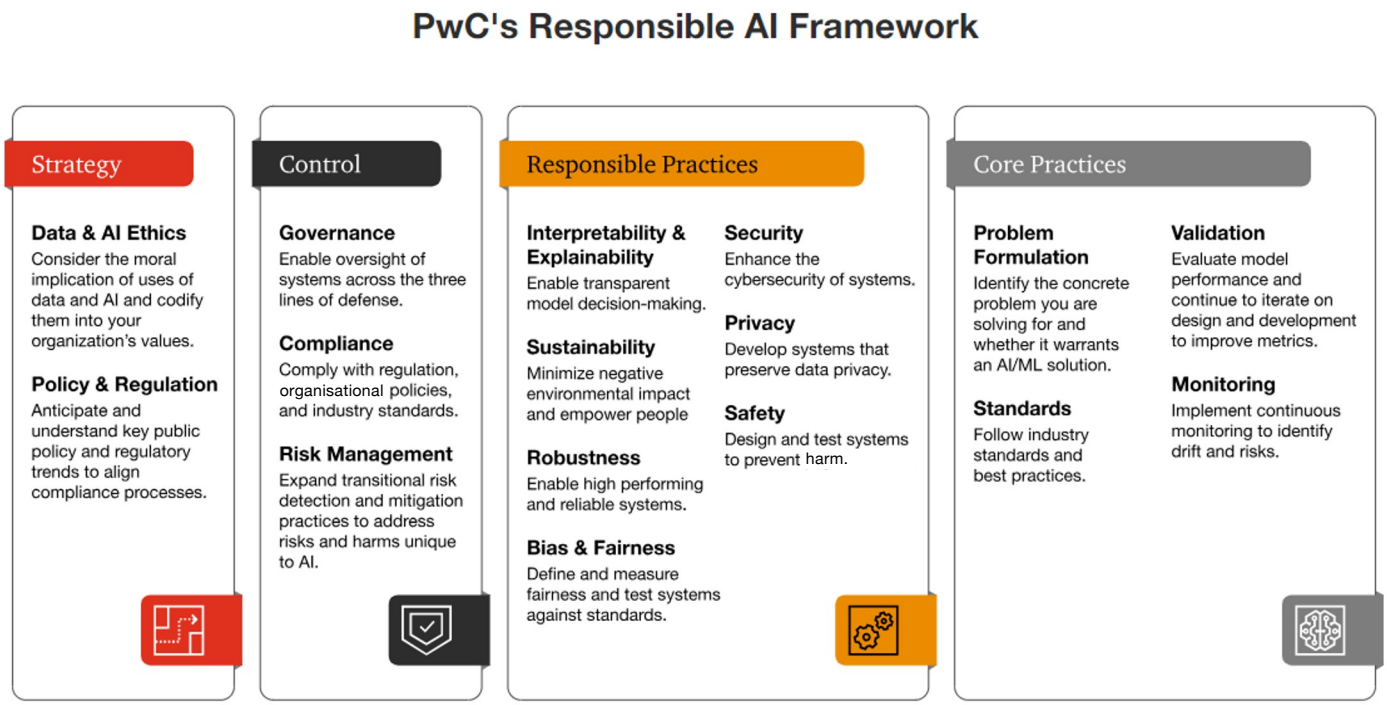
Effective AI governance begins with establishing the organisation's risk appetite for the use of AI. There is a delicate balance of moving swiftly but safely in relation to the adoption of AI. What's the company's appetite for risk when it comes to the use of AI, and what potential adverse consequences would the Board be willing to tolerate provided appropriate mitigations are in place?

Once this is defined, governance involves clearly defined internal organisational structures, roles and responsibilities, performance measures and accountability for AI outcomes that includes internal responsible stakeholders at a C-suite level.

A director's duty to act in good faith and for a proper purpose also extends to ensuring the AI governance framework considers the ethical implications of AI on the company. Adoption of AI must occur with an ethical mindset – consistent with the organisation's approach to business, its workforce, and data ethics.

There is a high use case for AI-augmented applications in workplace and workforce management. Not only is AI replacing certain roles in the business, but it is also making decisions about prospective workers and human capital management. Care must be taken by the company to ensure fairness, transparency and morality remain a stalwart to this use of AI – ethics will be critical in protecting the reputation and trust of any business moving forward.

An example of some frameworks and guidance in relation to implementing AI governance can be found in the PwC Responsible AI Framework and ISO/IEC 38507:2022 (further described on page 14). Having an effective AI governance strategy will be vital, and many people inside and outside of your organisation can influence your ability to use generative AI responsibly. They include data scientists and engineers; data providers; specialists in the field of diversity, equity, inclusion and accessibility; user experience designers, functional leaders and product managers.



5 Consider alignment with best practice AI risk management frameworks

Helpfully, there are a number of ethical AI and responsible AI risk frameworks/guidance which can form a useful base for any AI risk management framework.

These frameworks include:

- *ISO/IEC 23894:2023 - Information technology - Artificial intelligence - Guidance on risk management (further described on page 13)*
- *EU AI Act risk based regulation approach*
- *NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0)*
- *US Department of Energy – AI Risk Management Playbook*
- *Microsoft Responsible AI Standards.*

The NIST Artificial Intelligence Risk Management Framework provides helpful direction and guidance to companies to improve their AI risk posture. It is designed to 'incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems'.

The appropriate framework for your business will differ depending on your organisation's scope/use of AI tools and its risk appetite. The board should ensure that it is appropriately briefed by the business and subject matter experts in order to consider the appropriate framework to align the business against.

For further information on best practice risk management in the AI space, see 'Additional Sources' on page 17.

ISO standards are already here…

The International Organisation for Standardisation has already developed key standards in relation to AI governance and risk management, which any director should be aware of:

ISO/IEC 38507:2022
Information technology - Governance of IT - Governance implications of the use of artificial intelligence by organisations

ISO/IEC 22989:2022
Information technology - Artificial intelligence - Artificial intelligence concepts and terminology

ISO/IEC 23894:2023
Information technology - Artificial intelligence - Guidance on risk management.

ISO/IEC 38507 – AI governance

The standard covers the governance and management of AI, including the development of relevant policies and procedures (e.g. on use of data, culture and values, decision-making involving AI), and how to manage key stakeholders.

Crucially, the standard reinforces the importance of human oversight and accountability in the use of AI systems. It establishes the need for clear risk management processes, focusing on accountability, reputation and trust, duty of care, safety, security and privacy of data/information for both current and future uses of AI.

The standard applies to all organisations, including public and private bodies, government entities, and not-for-profit organisations, of any size irrespective of their dependence on data or information technologies.

Governance of AI is likely to develop as an additional duty of the board:

- As part of good governance, a framework should be in place to identify and manage AI risk.
- The framework should support tracking the development of existing AI risks and the emergence of new ones, as well as maintain a risk register which describes the steps taken to mitigate each risk.

6 Embed ongoing assurance of AI

AI is not set and forget. There is a need for an ongoing process to review and update the existing governance framework on a regular basis.

It is extremely important to set obligations around ongoing assurance, monitoring and testing of AI tools to ensure that they remain aligned with the organisation's business demands and obligations, as well as the requirement to meet changing technical specifications of AI and the needs of an evolving legal and regulatory landscape. Failure to do so may result in the degradation of AI model performance, also known as "drifting".

AI model drift occurs when the quality of the input data changes in a manner that lowers the accuracy of the AI prediction. In order to manage model drift, constant monitoring of the input data and the performance of the AI and its outputs is required. Directors must ensure there are suitably skilled company personnel checking data quality – where data quality has suffered, processes and procedures must be in place to retrain and fine tune the AI model to keep the model quality high.

Good governance practices spearheaded by the companies' directors and boards need to be agile. Appropriate care and diligence in discharging directors' duties calls for continued compliance with emerging legislation as it develops. Organisations should, therefore, implement routine health checks e.g. system reviews and auditing of data fed into AI models/systems to ensure it abides by all relevant privacy obligations and other local regulatory regimes.

Crucially, assurance in AI must be imported into every level of a business. There should be streamlined reporting from the operational functions to the board on AI implementation and use. Examples of such assurance reports would include (but not limited to) reports on any potential or current risks, user issues, security, and ethical concerns with AI.

Other considerations – can company directors use AI?

Robo-directors? AI in the boardroom

AI tools now have the ability to synthesise vast amounts of raw data in order to undertake various corporate exercises, for example, legal or commercial due diligence. These tools are becoming more mainstream when it comes to organisational decision-making. For example, a Hong Kong venture capital firm relied on an AI function to vote on an important financial investment decision for the company.[11] The computer algorithm was required to make a recommendation based on its analysis of significant amounts of market data.

This prompts the question as to whether AI can replace decision makers or even directors entirely? Under current New Zealand law, AI software could not be appointed as a director as the law requires a director to be a natural person. However, it isn't impossible to imagine a future world where this may be permitted (as observed above in Hong Kong). In fact, as AI technology becomes more widely-adopted and prevalent within organisations, directors may even be expected to use these tools in order to properly discharge their obligations.

However, at this stage, a director who would propose to make decisions within their organisation relying entirely on AI, without turning their mind to the decision itself and considering surrounding information and facts, such director may be exposed to liability for breach of their duties of care ultimately by reason of reliance on, or misuse of, AI. In essence, directors must always exercise the care, diligence and skill that a reasonable director would exercise in the relevant circumstances, and if relying on expert advice, must make proper inquiry where needed.[12]

AI is simply a tool that directors may use to assist their decision making but ultimately it should not replace the role of a director in its entirety. A director should always turn their mind to the output of various AI tools before making a final decision.

ESG and AI

AI has a real potential to revolutionise our approach to major global challenges. Many companies have begun using AI to promote ESG practices, e.g. climate change modelling, fintech solutions to provide access to affordable financial services, energy management, etc. However, companies should also consider the potential ESG downsides of implementing AI to ensure that its use results in a net positive ESG outcome. For example:

- Lack of transparency in AI processes leads to inability to properly assess exact ESG impacts of AI-related investments. ESG-focused investors depend on the information they are provided to ensure true change.
- In some circumstances, use of AI algorithms and data storage centres can increase the carbon footprint and energy consumption of a business. AI systems can require significant computing power to train large neural networks which may pose a threat to current ESG goals.
- As detailed earlier in this article, there is a real possibility of social discrimination and unethical outcomes in the implementation of AI models, if the right safeguards and controls are not in place for model design, model verification and ongoing model management.
- From a governance perspective, a key issue is a lack of technologically skilled staff from operational employees to those at the senior management level. As such, it is critical for directors and boards to upskill in AI, and ensure their organisation implements upskilling across the business.

11 BBC, *Algorithm appointed board director* (Web Page, 16 May 2014) <https://www.bbc.com/news/technology-27426942>.
12 *Companies Act 1993,* ss 137-138.

Key contacts

In today's fast-moving world, it's more important than ever to have a legal partner who understands all aspects of your business. A legal partner to help you move ahead effectively and decisively, to see today's challenges through a wider business lens and then uncover tomorrow's opportunities.

Mainstream use of artificial intelligence (AI) exploded onto the scene with ChatGPT and given the myriad of commercial applications for generative AI, it is looking like it is very much here to stay. As a result, many agencies and businesses are looking to embed AI into their day-to-day operations. But in amongst the plethora of legal, commercial and risk issues related to AI, where do you start? How do you accelerate responsibly? Please contact any of our team listed below to discuss how PwC can assist your organisation with your AI journey…

Kylie Reiri I Partner
Analytics, AI and Manukura
PwC New Zealand
T: +64 210 243 3589
E: kylie.a.reiri@pwc.com

Tom Logan I Partner
Corporate and Commercial Law
PwC New Zealand
T: +64 27 531 9282
E: tom.x.logan@pwc.com

Robyn Campbell I Partner
Cyber Consulting
PwC New Zealand
T: +64 27 592 1352
E: robyn.k.campbell@pwc.com

Chris Baldock I Partner
Workplace Law
PwC New Zealand
T: +64 21 474 321
E: chris.p.baldock@pwc.com

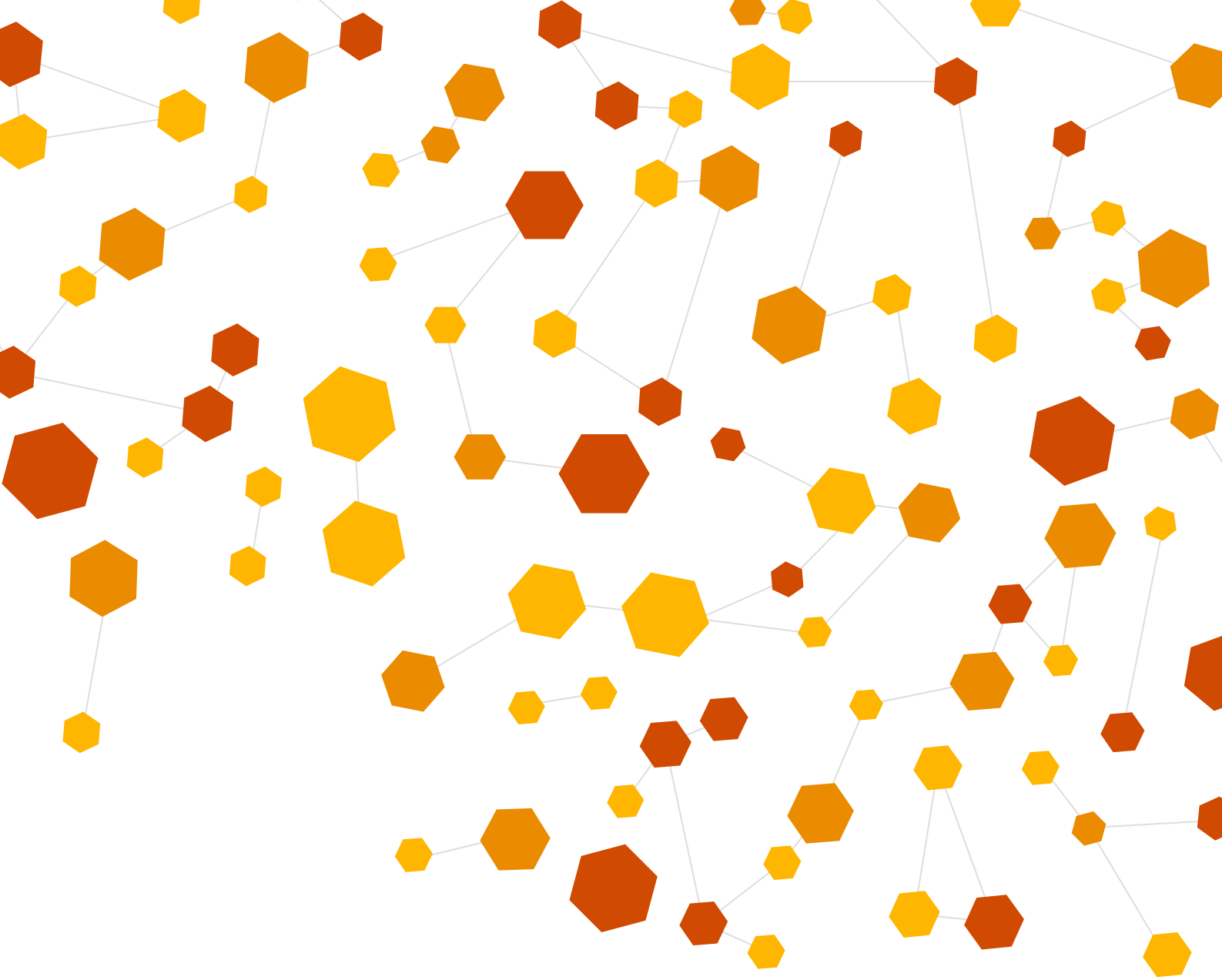
Nouras Hassan I Partner
Risk Services
PwC New Zealand
T: +64 210 708 823
E: nouras.b.hasan@pwc.com

Polly Ralph I Director
Privacy & Data Protection Law
PwC New Zealand
T: +64 27 374 2031
E: polly.k.ralph@pwc.com

Matt Keenan I Partner
Corporate and Commercial Law
PwC New Zealand
T: +64 21 834 216
E: matt.p.keenan@pwc.com

Gabrielle Wilson I Associate Director
IP Law
PwC New Zealand
T: +64 210 263 6450
E: gabrielle.x.wilson@pwc.com

- Insights for Non-Exec Directors: https://www.pwc.co.nz/communities/non-executive-director-insights-centre.html
- Managing the risks of AI: https://www.pwc.co.nz/services/risk-services/managing-the-risks-of-generative-ai.html
- PwC's Responsible AI Framework: https://www.pwc.co.nz/services/risk-services/what-is-responsible-ai.html
- Generative AI tools: https://www.pwc.co.nz/services/risk-services/generative-ai-tools-push-new-boundaries-for-responsible-ai.html



A community of solvers coming together in unexpected ways to solve the world's important problems

www.pwc.co.nz

pwc