AI procurement checklist

When deciding on a supplier to use, and developing related agreements, contracts or other documentation with those suppliers, ensure you understand:

- ☐ supplier reputation (including any published infringement claims), capability, legal compliance, pricing, and contract value

- ☐ alignment with your business needs and criteria

- ☐ alignment with the purposes and principles set as part of your AI governance approach

- ☐ whether training data meets your business's, and other required, standards (including, eg, that it is relevant to New Zealand, or that it was lawfully sourced)

- ☐ supply chain and security risks, including the potential to fail or be misused/attacked and any incident response plans

- ☐ where operational and/or input data is stored, and how it is protected, retained, used and destroyed

- ☐ model performance results (including around its accuracy and bias) and how it will be monitored and maintained

- ☐ ownership of model outputs and input data

- ☐ supplier terms of service/use, including for example around data governance and intellectual property. Consult industry peers, experts, or prior evaluations of the system to better understand system performance and any risks to consider.

- ☐ cost analysis – AI tools are presenting new commercial models and have different cost drivers to other known software models. Volume may be less relevant than computational chargers, which may not be fully transparent. Users need to be aware of and alert to the total cost of the tool and the impact of high usage, as well as the cost of ongoing support

- ☐ the risks of 'vendor lock-in' and how they will be managed, ensuring you understand if you can change providers, and whether its data is able to be easily migrated with any change.

- ☐ capacity to deploy the system and integrate with existing business systems and tools

- ☐ what support arrangements with the provider would be in place should something go wrong

Deployers or developers of AI systems should in turn offer to share the following information with their suppliers of AI systems, models, or components:

- ☐ expected use of the AI system, model or component

- ☐ where data privacy is a consideration, as much information as possible to highlight the issue and replicate the outcome without compromising data privacy or security such as data profiles or sample synthetic data

- ☐ issues, faults and incidents that occur with the system

- ☐ a schedule of regular reviews and updates of this information.

For more details and tips, Responsible AI Guidance for Businesses is available at mbie.govt.nz

11770 AOG