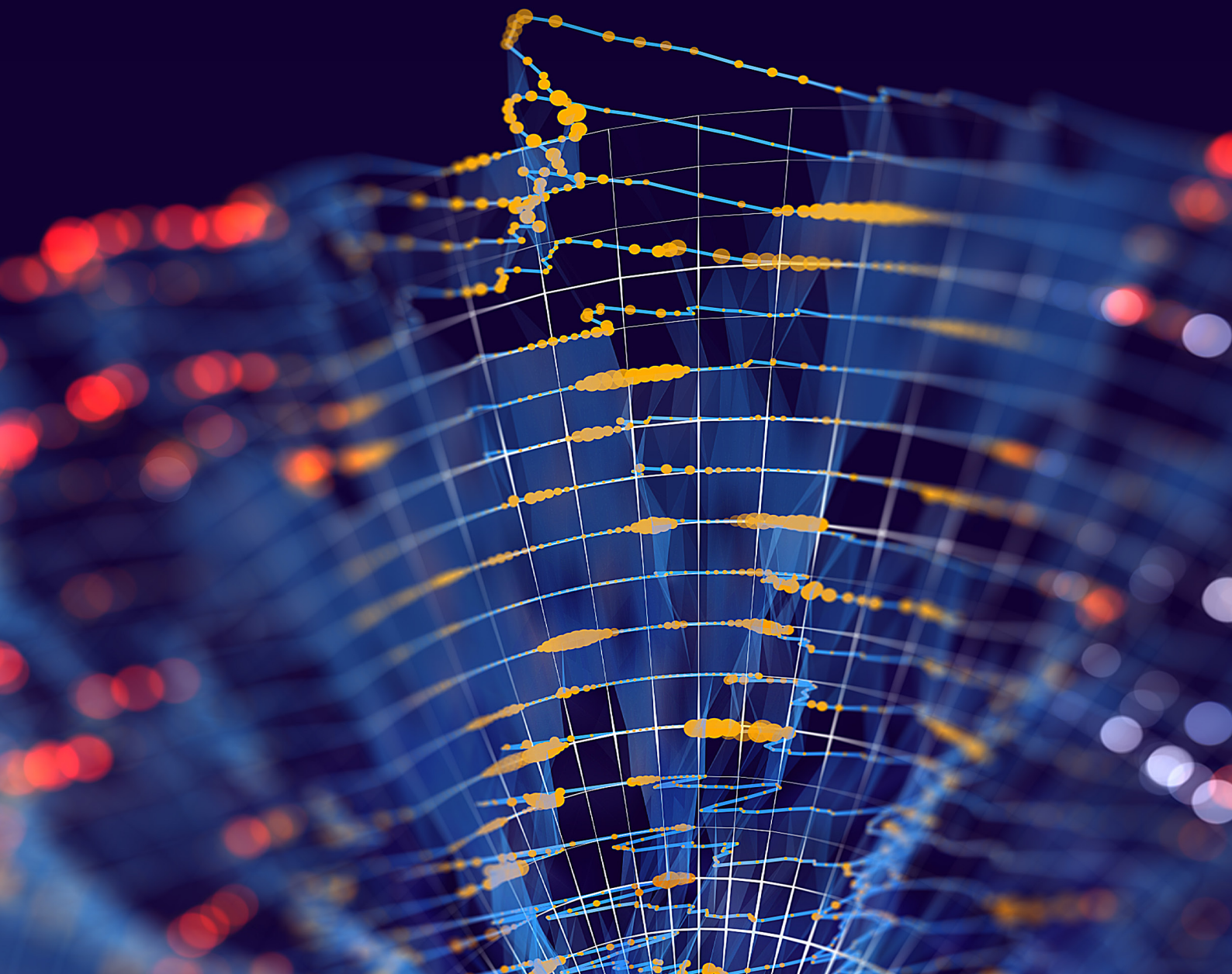
Queensland Government

FRONTIER SI

Governance in the Age of AI: Readiness and Responsible Leadership

Authors:

Dr Jia-Urnn Lee, FrontierSI
Gavin Kennedy, FrontierSI
Mark Gordon, Geological Survey of Queensland
Dr Rob Chatterjee, Geological Survey of Queensland
Steven Bowden, Geological Survey of Queensland



Acknowledgements

The Geological Survey of Queensland and FrontierSI respectfully acknowledge the Aboriginal and Torres Strait Islander people of Australia, first custodians of the lands, air and waters that sustain the places we live, work and play.

These first peoples have had a vibrant, living culture that has remained in sustainable synergy with the natural environment for tens of thousands of years, and continues to do so.

We pay our respects to Elders past, present, and emerging.

The authors acknowledge the contributions of Professor Flora Salim and Dr Aditya Joshi of the University of New South Wales AI Institute.

Creative Commons License

Citation

GSQ (2025), Governance in the Age of AI: Readiness and Responsible Leadership, October 2025.

Contents

1 Introduction

Artificial Intelligence (AI) technologies, in particular Generative Artificial Intelligence (GenAI), are rapidly transforming how the public sector, industry and research create, interpret and apply information.

In the domain of mineral resource exploration, AI promises to unlock insights from vast troves of data and create new efficiencies for exploration companies, alongside regulatory, research, finance and public stakeholders. However, the deployment of AI-enabled services within the public sector raises complex challenges, including trust issues of ethics, quality, reliability and explainability.

For an organisation or government department seeking to deploy a public facing AI-enabled service, these issues are compounded by the need to integrate such services into existing digital ecosystems and policy frameworks that are still adjusting to the AI revolution. Many future services are still at the Proof-of-Concept stage while these issues are addressed. While the value of these services is increasingly clear, the critical question is whether the organisation or government department is organisationally, technically, and ethically prepared to deploy these services responsibly and at scale.

This paper seeks to address that readiness gap. Drawing on the experience of the Digital Librarian Proof-of-Concept (PoC) led by the Geological Survey of Queensland (GSQ), it proposes two key tools for assessing and strengthening organisational capability to deploy AI-enabled services in complex, data-intensive domains such as resource exploration.

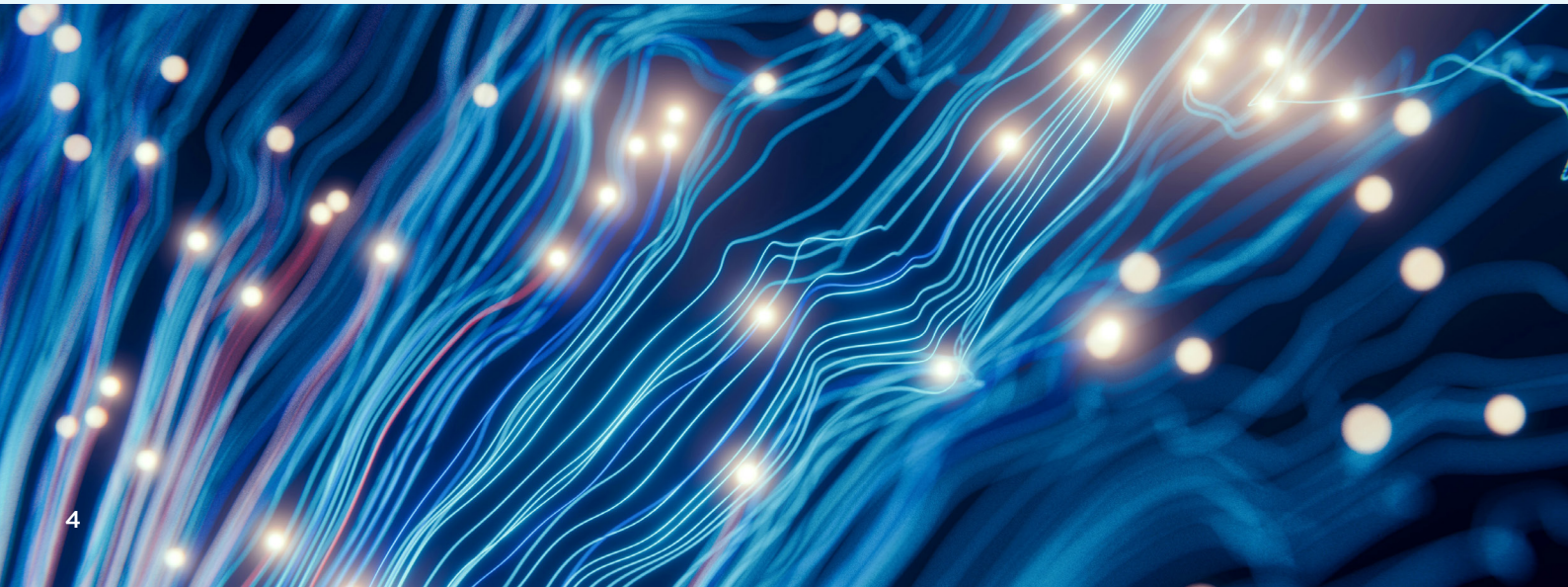
The **AI Business Readiness Framework** is a practical tool aligned with the AI delivery lifecycle, illustrating the domains (strategy, organisation, data, and technology) that require focus at each stage of AI implementation. It is designed to enable organisations to sequence investments and capability-building efforts in the right areas at the right time, ensuring a balanced and scalable approach to AI adoption.

The **AI Capability Delivery Governance Model** is designed to build on existing data governance structures, while embedding AI-specific roles, outputs, and risk management processes. The model ensures that AI adoption aligns with organisational goals and functions and broader corporate obligations while supporting responsible and ethical use of AI technologies.

Importantly, both tools are designed to be flexible and scalable, enabling any organisation to adapt and right-size it to their own needs and use cases.

This paper captures the innovative approaches and lessons learned following the Digital Librarian PoC through GSQ's collaboration with FrontierSI and the UNSW AI Institute. By shifting the focus from technical readiness to a comprehensive governance model, it offers valuable insights for government departments and organisations seeking to implement and deploy AI technologies responsibly and effectively.

As the field of AI continues to evolve, this work represents a snapshot in time, offering a contribution to the ongoing refinement and innovation of AI-enabled services. By sharing these insights, we aim to contribute to the broader conversation on AI readiness, supporting organisations in unlocking the full potential of AI-driven solutions.



2 Background

2.1 Why we did this

The Geological Survey of Queensland (GSQ), as the custodian of Queensland's geoscience knowledge and data, plays a pivotal role in supporting the sustainable exploration and development of the state's mineral and energy resources. However, the resource exploration landscape is becoming increasingly complex, with fewer greenfield opportunities, stricter regulations, and heightened social and environmental considerations.

A key challenge faced by the resource exploration industry is the difficulty in accessing and integrating vast and complex geological datasets. This challenge presents itself to resource exploration companies in two ways: they may lack the capacity, in terms of capital and/or labour, required to efficiently locate, analyse, and extract actionable insights from disparate historical datasets, or they may lack the specialised tools and workflows necessary to do so. From the point of view of the resource exploration company, this can lead to suboptimal decision-making, higher exploration risks and missed opportunities.

To address these issues GSQ initiated the Digital Librarian Proof-of-Concept (PoC) to explore the potential of Generative AI (GenAI). By leveraging Large Language Models (LLMs) and Retrieval-Augmented Generation (RAG) tools, the PoC demonstrated how GenAI could streamline data discovery, enabling explorers to quickly access relevant information across large volumes of reports to make smarter, data-driven decisions.

While the PoC demonstrated early technical successes, it also raised an important question: *could GSQ operationalise and adopt AI at scale, and if so, how?* To explore this, FrontierSI and the University of New South Wales (UNSW) AI Institute were engaged to collaborate with GSQ to evolve the Digital Librarian concept into an operational, industry-focused service. The team conducted stakeholder interviews across industry, academia, and government, and assessed a range of aspects including benefits, governance requirements, AI readiness, and technology architectures.

The resulting recommendations were initially targeted for internal Queensland Government consumption. However, many aspects of this work are novel and shed new light on how AI tools can be practically integrated into organisations, particularly:

- Assessing business readiness, not just from a technical perspective but also from strategic, organisational and data perspectives.
- Applying governance measures holistically and progressively, reflecting both the level of risk and the stage of AI lifecycle development.

This white paper focusses on ideas and concepts applicable to organisations wishing to adopt generative AI in a similar way to what GSQ is proposing, by:

- Articulating the value proposition of a GenAI-enabled tool to GSQ, provided here for geoscience data discovery as introductory context.
- Presenting the findings from our assessment in this whitepaper, which have broad applicability to other AI-enabled service activities, particularly addressing governance and business readiness.

This work is ongoing and as such represents a snapshot in time as both GSQ and FrontierSI continue to further develop the ideas and concepts presented here.

2.2 From data modernisation to GenAI

GSQ's data modernisation journey has laid strong foundations for digital innovation in resource exploration, with significant opportunities still to be realised. As shown in Figure 1, by examining the enablers, outcomes, and limitations of current approaches, the case emerges for GenAI as the next step in transforming data discovery and strengthening the competitiveness of Queensland's resources industry.

Current State: GSQ Data Modernisation

Enablers:
- Keyword or spatial search e.g. through Open Data Portal
- Established metadata standards
- Trusted source for industry

Outcomes:
- Returns location of individual reports
- Visualisation of results

Limitations:
- Users analyse data and derive insights manually
- Time-intensive data gathering

Breakthrough

Evolving from finding individual reports to discovering hidden patterns across QLD's geological knowledge base

Foundation established: AI-enabled, automated cross-report analysis

Proof-of-Concept: Digital Librarian

Enablers:
- GenAI reads geological reports
- 2900 reports
- Users ask questions via natural language query

Outcomes:
- Digital Librarian returns insights from reports
- Rapid information synthesis

Limitations:
- Cannot handle non-text data
- Accuracy and reliability concerns
- Not enterprise-integrated

Transformation

Transforming how exploration companies work – from data hunting to strategic analysis and GenAI-enabled geological intelligence

Validated concept: ready for production planning and design

Future State: GenAI-enabled tool

Enablers:
- Enterprise-ready AI integration
- Search from GSQ repository
- Natural language & spatial queries
- Multi-modal AI-enabled insights

Outcomes:
- Faster target-to-drill for junior companies
- Industry trusts use of GenAI in exploration
- Queensland Government sets standard for AI-enabled critical minerals exploration

Figure 1: Evolution of GSQ's geological data discovery capabilities and offerings, from current state via the Digital Librarian proof-of-concept to the envisioned future state as a GenAI-enabled tool.

2.2.1 Current State: GSQ Open Data Portal

GSQ has been the custodian of geological data, reports, scientific surveys and resource commodity information for over 150 years.[1] In 2020 GSQ uplifted their data ecosystem to enhance data access and reporting services. A key component of this modernisation effort was the GSQ Open Data Portal[2] (ODP), which now provides access to over 184,000 datasets exceeding 70TB of data. These include statutory industry reports lodged by exploration and mining companies to report on exploration activities, which are made publicly available after a mandatory confidentiality period.

Enablers: Established data quality and management to enable keyword and metadata search.

Outcomes: Users such as explorers and operational teams can quickly find individual reports.

Limitations: Despite these advances with the ODP, users can experience time-consuming searches connecting disparate information across reports and complex datasets, making it difficult to convert these data into integration-ready insights.

A generative AI-enabled solution to the above limitations could be transformative in accelerating data discoverability in Queensland's mining and energy industries. A forward-looking generative AI approach would:

- Streamline discovery by providing targeted access across vast, complex datasets.
- Simplify workflows and generate insights in usable formats, facilitating faster exploration to target times.
- Leverage existing investment by incorporating GenAI into GSQ data portals, maximising benefits and strengthening industry engagement.
- Address modern challenges by integrating larger and more diverse datasets, improving transparency, and addressing declining discovery rates in exploration.
- Attract investment by positioning Queensland as a premier exploration destination with trusted, accessible data that reduces risk and accelerates decisions.

2.2.2 Generative AI Proof-of-Concept

The challenges and limitations of data discovery, coupled with the possibilities of leveraging rapidly emerging AI technology, led GSQ to conceptualise the Digital Librarian which served as a PoC to assess how users of ODP data could analyse, interpret, and extract value from unstructured data.

Enablers: The PoC used LLM and RAG tools to query unstructured data within reports and allow plain language questions via written prompts.

Outcomes: It showed that such a service could deliver insights that are otherwise not accessible through existing metadata-enhanced keyword searches and text-based deep learning models, while overcoming challenges like inconsistent data formats and domain-specific language.

Limitations: The PoC was limited to handling text-based data, with concerns about output accuracy, reliability, and alignment of AI policies and principles. As a PoC it was not integrated into the ODP, or into Queensland Government enterprise or corporate governance frameworks.

2.2.3 Translating policy into action

In envisioning a future-state GenAI-enabled tool for data discovery, the major question for GSQ was how to undertake this within the Queensland Government context.

At the time of the PoC development, the Queensland Government Artificial Intelligence governance policy[3] was just released. Various other policies and frameworks emphasised the need for strong governance and robust risk assessment for responsible and ethical AI adoption, however they offer limited practical guidance on how to translate these principles into an implementable framework. The following sections present the practical recommendations that respond to this policy gap by introducing a business Readiness Assessment Framework, a Governance Framework, and broader lessons from the Digital Librarian initiative to guide responsible, scalable AI adoption.

[1] Data Modernisation in Geological Survey of Queensland. www.data.qld.gov.au/article/case-studies/data-modernisation-in-gsq.

[2] GSQ Open Data Portal. https://geoscience.data.qld.gov.au. The Open Data Portal comprises 70TB+ of geophysical surveys, geochemistry data, geological maps, borehole logs, and exploration reports, while supporting comprehensive metadata search, geospatial visualisation and interface functions.

[3] Queensland Government Artificial Intelligence Governance policy. www.forgov.qld.gov.au/information-technology/queensland-government-enterprise-architecture-qgea/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/artificial-intelligence-governance-policy.

3 An AI Readiness Assessment Framework

An AI Readiness Assessment Framework was designed to evaluate how prepared an organisation or department is to adopt AI technologies such as the GSQ GenAI-enabled tool.

3.1 Core domains of AI readiness

Effective AI adoption requires readiness beyond technology maturity. Strategy, organisation, data, and technology form the foundations of AI readiness, ensuring adoption and use is responsible.

Strategy ensures alignment and governance for responsible AI development and use.

Organisation ensures leadership, capability, and capacity to deliver and sustain AI initiatives.

Data ensures trust, integrity and quality as the foundation for AI systems to perform.

Technology ensures the infrastructure, models and tools needed for implementation and delivery are fit for purpose.

These domains overlap within a Venn diagram (Figure 2), illustrating how different elements of readiness interact. This visual model highlights the importance of addressing not just the individual domains but also their intersections, which reflect essential aspects of AI-readiness.

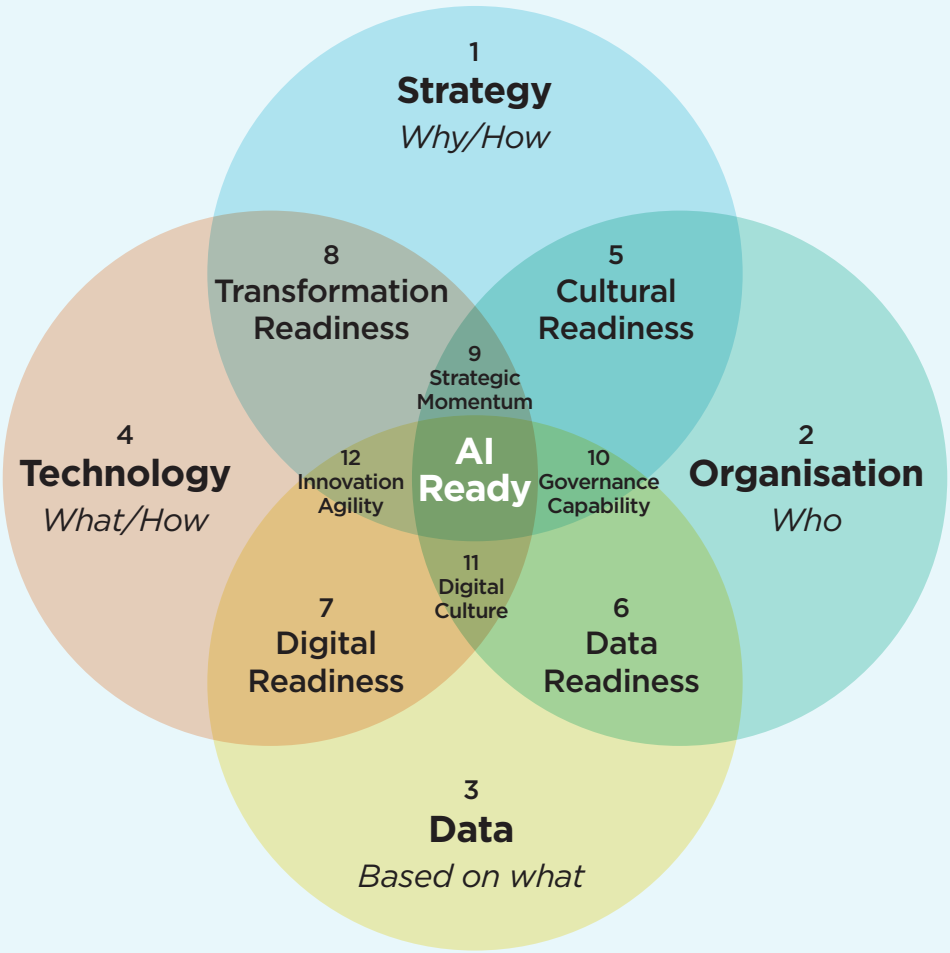


Figure 2: Multi-domain AI-readiness framework, anchored by Strategy, Organisation, Data and Technology.

Each of the domains and their intersections are made up of the considerations in Table 1.

Table 1: Breakdown of AI readiness domain components.

1. Strategy

- Comprises strategy, accountability, governance, and alignment with organisational and enterprise strategy.
- Why are we doing this?

2. Organisation

- Comprises culture, business, workforce, stakeholder buy-in, use case readiness.
- Business capacity, capability
- Who are we solving this for? Who will do it?

3. Data

- Data as the foundation that technology is based on, or informed by.
- What is the technology based on?

4. Technology

- Technological and digital maturity.
- What are we using?
- How will we use or be informed by other drivers?

5. Cultural Readiness

- Leadership is committed and works to align AI use case maturity with strategy.
- Strategies for people and talent are aligned with long-term AI goals.
- Shared ownership and accountabilities across departments and business units.

6. Data Readiness

- Data stewardship.
- Organisation has the skills, resources, and attitude to use data tools and outputs.
- The organisation supports processes and training that encourages effective data use.

7. Digital Readiness

- Integration of AI, data, and infrastructure technology to support intended use cases.
- Interoperable, scalable solution architecture enabled by data architecture, and leverages platform access, reuse, and integration.

8. Transformation Readiness

- Aligning emerging technology with broader strategic and policy objectives.
- Aligning external shifts in technology with longer-term policies, strategies, and intended outcomes.

9. Strategic Momentum

- Organisational culture embraces innovation and supports timely action to implement AI projects and programs.

10. Governance Capability

- Translating vision into implementable AI plans.
- Developing the structures, protocols that can support development and AI adoption.
- Governance to ensure technology investments meet business needs.

11. Digital Culture

- Embedded culture of collaboration across business needs, user needs, and delivery.
- Shared ownership of processes and outcomes among cross-functional teams.

12. Innovation Agility

- Robustness and responsiveness in strategy to pivot or leapfrog to harness high-value data with the right technologies.

3.2 What good looks like

To meaningfully assess AI readiness, organisations need to understand what "good" looks like, how progress can be gauged, and where to focus effort. The following sections describe each domain, outlining why they exist, how readiness is considered, and select criteria against which AI readiness can be gauged. For more detailed criteria, including prioritisation and recommended metrics, please refer to Appendix C: Assessment criteria. For a discussion on the AI lifecycle states, please refer to Section 4.2 Alignment with AI Lifecycle Stages.

STRATEGY

What: The Strategy domain anchors the responsible governance, accountability, and adoption of AI.

Why: This domain ensures AI implementation and utilisation is led from the top, aligned with organisational priorities, and supported by governance frameworks consistent with (in this case) public sector legislation.

Readiness focus: Framework and controls should be fit-for-purpose, and applied proportionally to the scale, complexity, risk profile, and lifecycle of the AI-enabled service.

Guiding question: *"How are we doing this, and how are we ensuring it is done responsibly?"*

Strategy Readiness looks like:

- An endorsed AI strategy with clear alignment to organisational priorities.
- A governance framework that ensures accountability and scales with the AI lifecycle.
- Regulatory and legal obligations addressed from the outset.
- Risks and impacts proactively identified and managed.
- Ethical and human-centred values embedded, including fairness, transparency, privacy, and accountability.

ORGANISATION

What: The Organisation domain focuses on the leadership, workforce, and cultural readiness required to deliver, sustain and scale the AI-enabled service.

Why: Leadership and organisational readiness play a key role in aligning the direction of AI initiatives with the long-term priorities and strategies, communicating the use case, benefits, and investment justification.

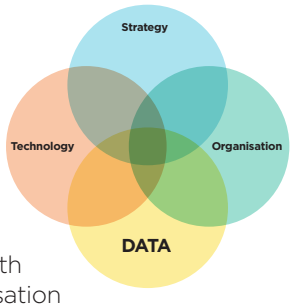
Readiness focus: Readiness is facilitated by stakeholder and change management, and enabled by workforce, business, and delivery capabilities, and cultural readiness to implement.

Guiding question: *"What is the problem we are solving, who are we solving this for, and who will deliver this?"*

Organisational Readiness looks like:

- Committed leadership that sponsors AI initiatives and aligns it with organisational or government priorities.
- Engaged stakeholders and change management processes that build trust, manage expectations, and prepare the workforce for AI adoption and development.
- A skilled and resourced workforce with the capacity, training and support to deliver and sustain the AI-enabled service.
- Robust business and financial foundations, including a clear business case and budgeting for long-term viability.
- Cultural readiness and digital literacy across the organisation to embed AI responsibly and at scale.

DATA



What: The Data domain focuses on ensuring data is available, accessible, high quality, secure and well-governed to support both the training and operationalisation of the AI-enabled service.

Why: It aligns technological capability with business needs, enabling integration into the broader organisational context.

Readiness focus: Readiness is assessed through the lens of trust, traceability, and integrity as the AI-enabled service matures through its lifecycle.

Guiding question: *"What is the data that is foundational to technology adoption?"*

Data Readiness looks like:

- High quality, complete, and reliable data with assurance processes to ensure accuracy, consistency, trustworthiness.
- Provenance and integrity controls to track data origin, verify authenticity, and protect it across its lifecycle in AI use.
- Robust security and privacy safeguards including access controls, encryption, and compliance with privacy requirements.
- Processes to detect and mitigate risks such as bias, drift, or malicious modification, ensuring data remains fit for modelling.
- Lifecycle governance for storage, use, and secure disposal of data, supported by regular risk assessments.

TECHNOLOGY

What: The Technology domain focuses on the digital, infrastructure, and AI technological capabilities required to deliver the AI-enabled service.

Why: It ensures technology is aligned with business needs and integrated into the broader organisational context.

Readiness focus: Readiness is assessed through the maturity of AI models and enabling infrastructure, with emphasis on scalability, reuse, and integration as the tool matures.

Guiding question: *"What are we going to do it with?"*

Tecnhology Readiness looks like:

- Agile, user-informed development processes with modular design and stage-gated processes,
- A clear product strategy that defines service performance, demand and future direction.
- Robust AI model management including validation, testing, monitoring, and fairness considerations.
- Fit-for-purpose infrastructure that is scalable, aligned with enterprise architecture, and shareable across initiatives.
- Scalability and service management plans that ensure the AI-enabled service can grow, integrate, and sustain performance over time.

3.3 AI readiness profiles

Purpose of the spider diagram

To support AI-readiness benchmarking a four-axis radar chart, or spider diagram, was developed around the Strategy, Organisation, Data, Technology domains. Each domain was assessed against foundation criteria and prioritisation (refer to Appendix C: Assessment criteria) to create the readiness profiles. This approach provides a baseline to support AI-readiness planning and highlights where uplift is required to support development and adoption of the AI-enabled service.

Using the diagram to guide investment and planning

The spider diagram provides a simple visual reference of how well the critical criteria are covered within each domain. This provides an accessible yet meaningful reference to support investment decisions, identify capability gaps, and ensure proportionality of effort in line with the intended use, scale, and risk profile of the AI-enabled service. The spider diagram shown in Figure 3 utilises GSQ's Digital Librarian PoC as an example to show both the current and desired states:

- Current state profile (**Gold**): Shows GSQ's relative strengths in areas such as Data (supported by the GSQ Data Modernisation effort) and Technology (supported by usage of AWS suite of tools for the Digital Librarian). In contrast, other domains such as Strategy and Organisation lag, assuming little to no formal GSQ AI Strategy or change management activities at the outset of this PoC.

  This profile underscores why the PoC, while successful, could not be scaled without broader organisational uplift. Profiles will differ across organisations depending on maturity.

- Desired state (**Blue** to **Green** profiles): These represent aspirational or future state readiness profiles at different stages of the AI lifecycle, where effort is distributed as appropriate across all domains, to uplift overall AI readiness.

  These profiles illustrate a pathway for GSQ and similar organisations to evolve beyond technology pilots and embed AI responsibly across Organisational, Strategy, and Data capability.

Lifecycle-aligned readiness view

The spider diagram can also be matched directly to the AI lifecycle stages (see section 4.2 for explanation of the Australian Cyber Security Centre AI Lifecycle Stages), with colour-coded overlays showing how AI initiatives progress across phases such as Stage 1: Plan and Design, Stage 3: Build and Use Model, and Stage 5: Deploy and Use, making it easier to anticipate and target priority next steps.

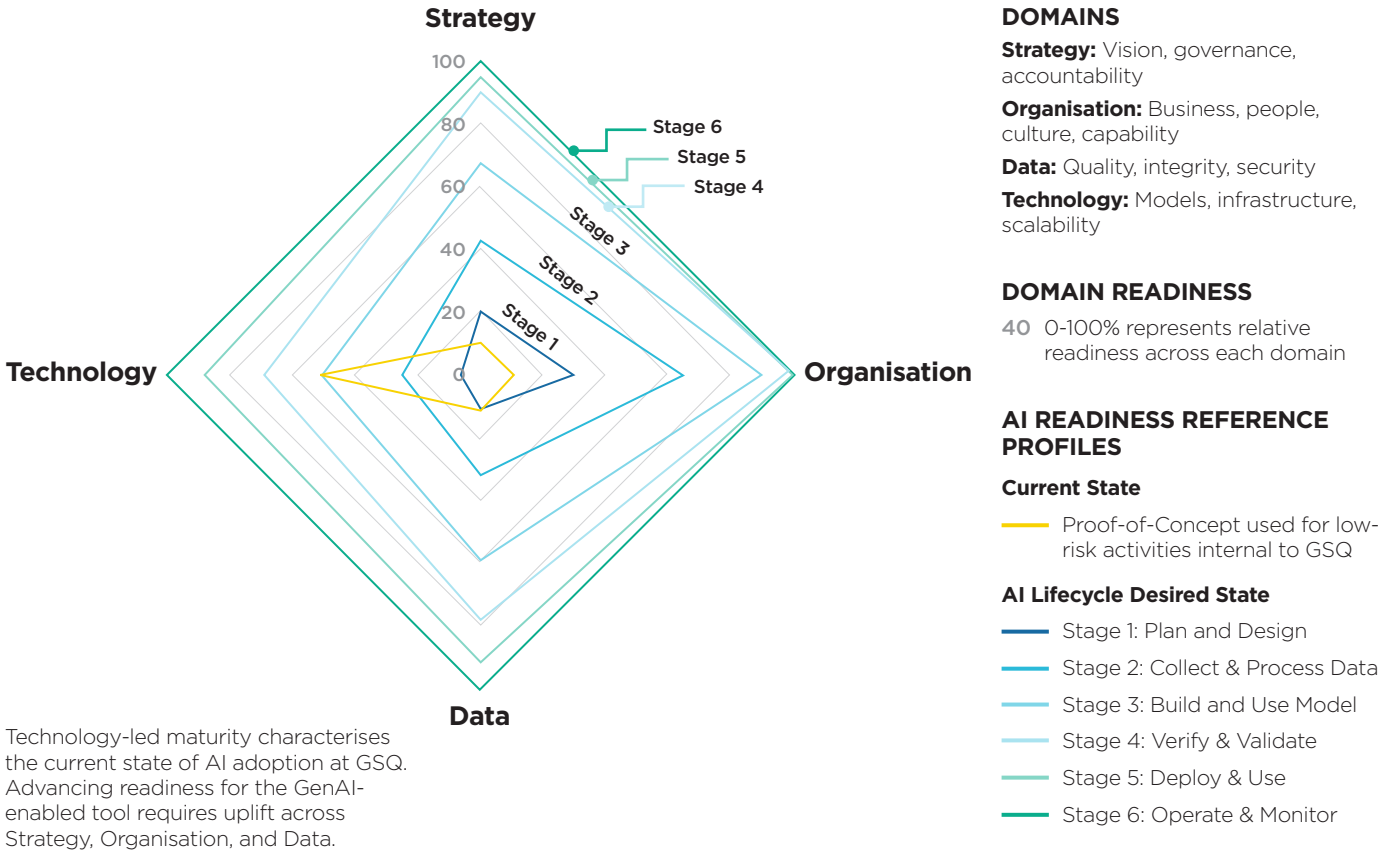
Limitations

The AI Readiness Assessment Framework remains high-level and was not intended as a full diagnostic of GSQ's current state or AI readiness. The framework and visuals – comprising the Venn diagram, criteria tables, and spider diagram – are a first iteration to be refined through implementation and validation with stakeholders.

As a next step, stakeholder engagement could confirm whether GSQ's current profile (gold profile in Figure 3), in the context of its Digital Librarian PoC, is broadly indicative of GSQ, or even of similar government agencies, and test its scalability as a continuous improvement tool.

Informing governance

The insights from the Readiness Assessment Framework provide the baseline for determining which governance artefacts are required at each stage of AI maturity. In this way, readiness assessment informs governance design, ensuring that governance is applied proportionately to risk, scope, and organisational capability.



Technology-led maturity characterises the current state of AI adoption at GSQ. Advancing readiness for the GenAI-enabled tool requires uplift across Strategy, Organisation, and Data.

AI Lifecycle Stages

Figure 3: Spider diagram visualising AI readiness profiles across lifecycle stages, showing how GSQ's current state compares to reference benchmarks and where uplift should be prioritised.

4 An AI Governance Framework

The governance processes and artefacts of the Digital Librarian PoC were intentionally minimal, adhering to a Queensland Government AI assessment (FAIRA[4]) and an internal GSQ review, which was considered appropriate for testing within a controlled environment with managed technology, data, personnel, and processes. However, transitioning to a production-ready, publicly accessible AI-enabled capability introduces higher risks, necessitating significantly enhanced governance and understanding of a government agency's overall readiness to deliver this capability.

In addition to the Readiness Assessment Framework, this section presents an AI Governance Framework to further support the productionisation of an AI-enabled service. This section also defines representative roles and responsibilities to ensure accountability and oversight during the AI-enabled service's lifecycle. This Governance Framework, while proposed for use within GSQ, is designed in a way that other government agencies and organisations may adapt to their own contexts.

Together, the two frameworks are intended to be complementary. The Readiness Assessment Framework identifies strengths and gaps across strategy, organisation, data and technology, while the Governance Framework translates these insights into practical roles, artefacts, and oversight mechanisms.

4.1 Enterprise-level AI governance

The national *Policy of Responsible Use of AI in Government*[5], which applies to both federal and state government agencies, mandates that government entities integrate AI considerations into existing governance frameworks. Best practice recommendations for organisational governance[6] support the position of AI governance alongside data governance. Using Queensland Government as a model, a brief overview of broad roles related to AI governance can be found in Table 2.

Area	AI function / roles
Corporate Governance	• Approves investment on digital initiatives including AI-enabled systems. • Develops AI policies and advises on implementation of policies to digital initiatives. • Provides guidance and assurance for Government agencies on how to evaluate use of AI for government business.
IT Governance	• Enterprise governance and architecture assurance for Government agencies • Advises on and ensures compliance with information and security matters in achieving the goals and objectives of the Government's information/digital strategies. • Advises on and ensures compliance with information and security matters in achieving the goals and objectives of the appropriate AI Policies.
Data Governance	• Custodian of data, reports, analyses and contextual information on which AI applications can be built for enhancing data discovery.
AI Governance	• Leads the realisation of the AI-enabled service • Ensures compliance with AI, IT and Data governance policies.

Table 2: Broad responsibilities within the Queensland Government related to AI.

[4] Queensland Government FAIRA Framework. www.forgov.qld.gov.au/information-and-communication-technology/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/faira-framework.

[5] Policy for the responsible use of AI in government. www.digital.gov.au/policy/ai/policy.

[6] Defining organizational AI governance. https://link.springer.com/article/10.1007/s43681-022-00143-x.

An AI governance structure was designed to build on the existing GSQ data governance framework, recognising the foundational role that data quality, integrity, and stewardship play in determining the outcomes of the AI-enabled service. The data governance framework focuses on the governance of foundational geoscience data and its associated data assets and artefacts. In its current form it does not explicitly incorporate AI governance elements.

Since AI systems are fundamentally data-driven, there will be a natural and necessary integration between data governance and AI governance functions. This cross-over will be evident in areas such as privacy protection, security, and data quality assurance, where existing measures can be extended to support responsible AI implementation.

4.2 Alignment with AI lifecycle stages

The AI governance structure comprises both organisation-level and product- or system-level components, mapped to the six AI lifecycle stages (Figure 4), based on the AI data security framework outlined by the Australian Cyber Security Centre[7].

The AI governance structure (Figure 5) includes a range of governance artefacts, being frameworks, strategies, and plans, introduced at different lifecycle stages. Their proposed usage can be scaled based on the risk profile and governance burden associated with either the type of AI initiative, or the maturity of a specific AI initiative, e.g. the GSQ GenAI-enabled tool from proof-of-concept through to future-state productionisation.

Figure 4: The six AI Lifecycle Stages.

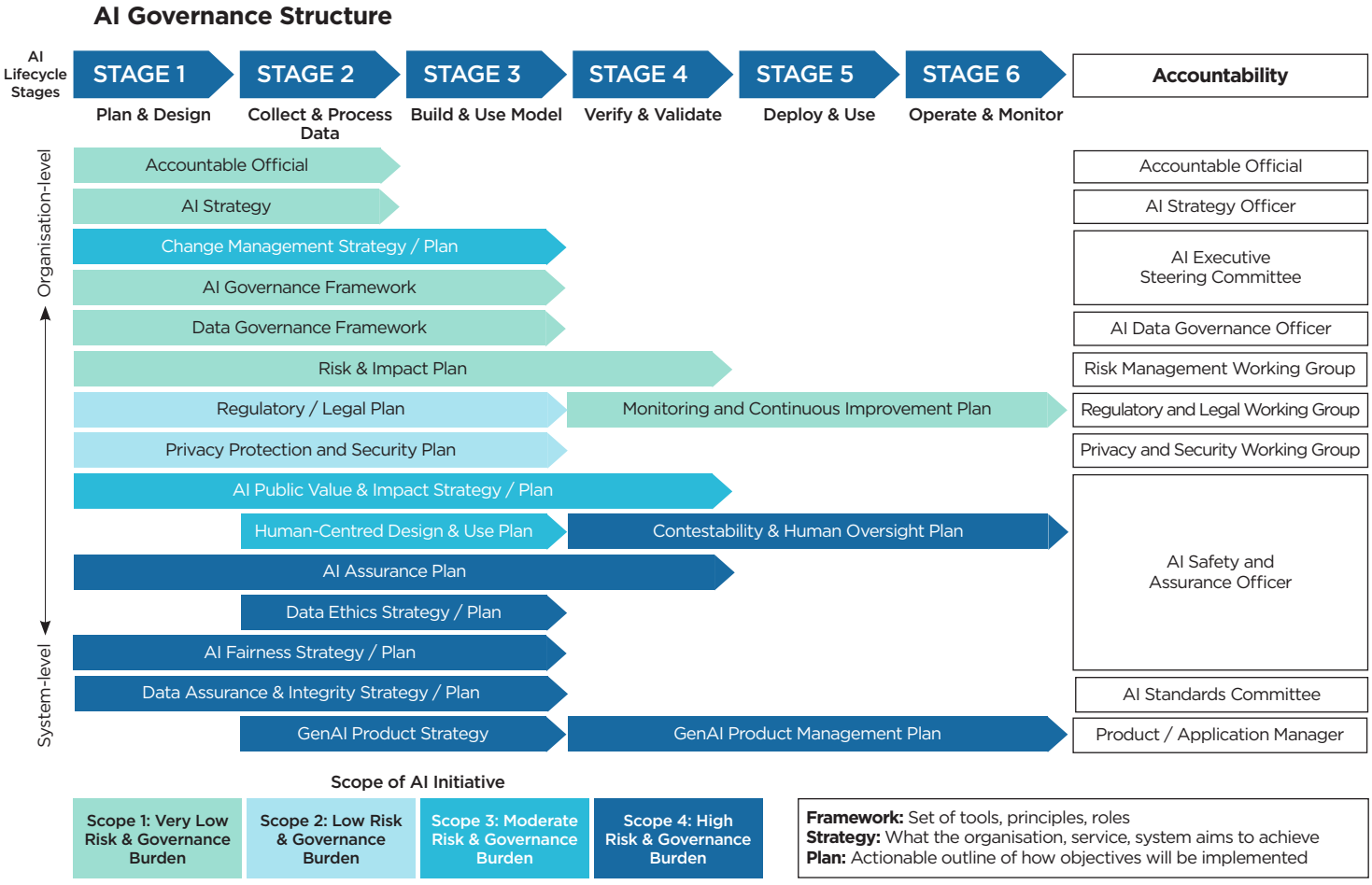


Figure 5: Representative AI governance structure for GSQ. The provisions for Scope 1-4 are described in text. Descriptions of the artefacts and accountabilities are provided in Appendix A and B.

[7] Australian Cyber Security Centre AI Data Security. www.cyber.gov.au/resources-business-and-government/governance-and-user-education/artificial-intelligence/ai-data-security.

These artefacts include foundational elements such as the Accountability Framework, AI Strategy, and AI Governance Framework, which are expected to be in place early, regardless of system complexity or intended use. Descriptions of each artefact are provided in Appendix A: Description of AI governance artefacts, and descriptions of accountabilities are provided in Appendix B: Roles, responsibilities and accountabilities.

4.3 Right-sizing by scope and risk profile

The governance structure is designed to be scalable and risk-proportionate, with adoption driven by assessed risk and scope of the AI system (Figure 6). It is also robust in that it can be adapted to accommodate the introduction of new AI systems and capabilities. It considers how scope and risk of the AI-enabled service influence the prioritisation and stage-gated implementation of the AI Governance Framework. Risk levels can be determined via an appropriate framework, in the case of Queensland Government this is the FAIRA Framework[8], alongside other relevant assessments (such as those for privacy, security, human rights and impact), and can be assessed from factors such as:

- Type of AI service (e.g. ranging from a low-risk consumer application to a more complex self-trained model[9]).
- Whether the AI system is intended for internal versus external use, impacting security, privacy, and trust.
- The use of confidential data repositories versus publicly available data only.
- Dependencies between systems, which may affect risk management.
- Isolation from other backend data sources and applications (e.g. sensitive or non-embargoed data systems).
- Conversely, clear isolation of the AI-enabled service as a non-integrated platform would reduce its governance burden.

The governance structure establishes a foundation for future planning and continuous improvement activities, such as defining maturity-model attributes and outcomes (e.g. as proposed in the Gartner AI Maturity Model[10]) to define an optimum state for the components of the Governance Framework.

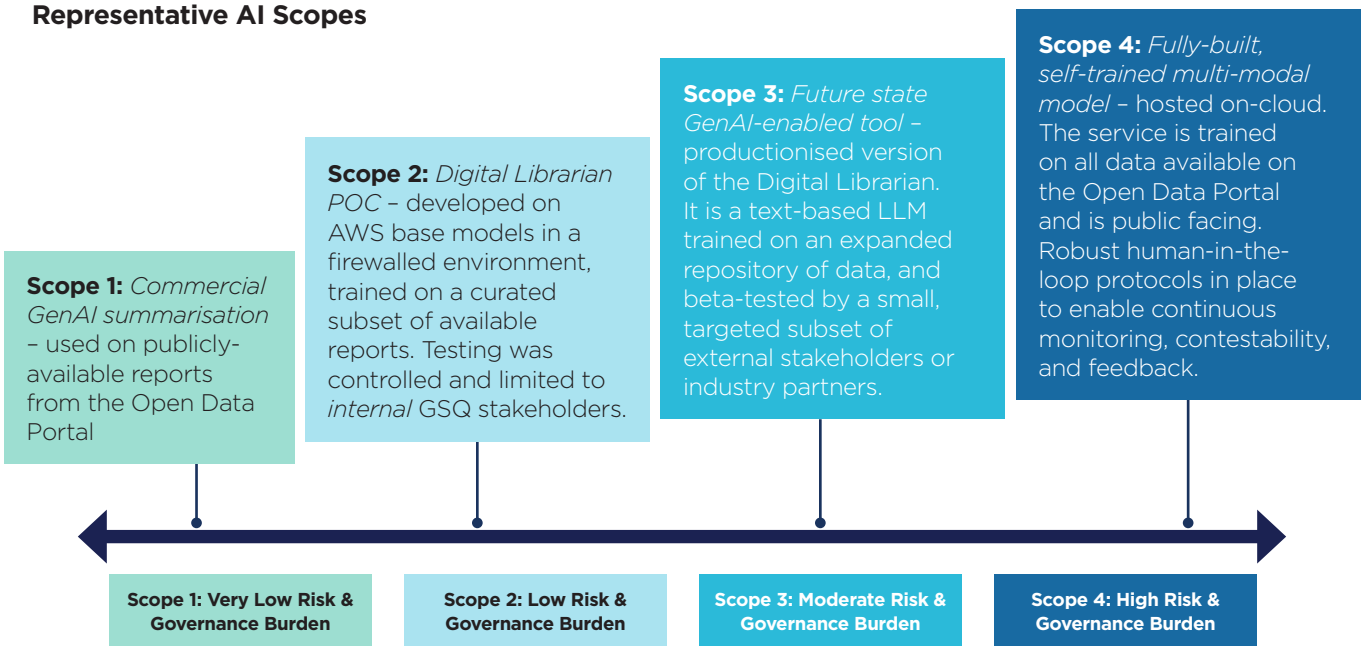


Figure 6: Representative AI use cases aligned to scope.

[8] Queensland Government FAIRA Framework. www.forgov.qld.gov.au/information-and-communication-technology/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/faira-framework.

[9] AWS, 2023. Securing generative AI: An introduction to the Generative AI Security Scoping Matrix. https://aws.amazon.com/blogs/security/securing-generative-ai-an-introduction-to-the-generative-ai-security-scoping-matrix.

[10] Gartner AI Maturity Model & Roadmap Toolkit, 2025. www.gartner.com/en/chief-information-officer/research/ai-maturity-model-toolkit.

4.4 Practical application

As shown in Figure 5 and Figure 6, governance is tiered from Scope 1 (very low risk and very low governance burden) through to Scope 4 (high risk and high governance burden), guiding which artefacts are required or optional, and at which stages of the lifecycle they are established. For instance:

- An Accountability Framework or Risk and Impact Management Plan would be necessary, regardless of the AI system's scope.
- A Scope 2 product requires all Scope 1 artefacts to be developed, as well as a Regulatory and Legal Plan, and a Privacy Protection and Security Plan. Example use cases for the GSQ initiative are represented along a qualitative scope and risk spectrum illustrated in Figure 6. For instance, the Digital Librarian PoC may be considered a Scope 2 product (i.e. low risk), requiring Scope 2 levels of AI governance (i.e. low governance burden).
- A Scope 4 product would require all previous Scope artefacts to be developed, as well as a Contestability and Human Oversight Plan. The need for human oversight or human-in-the-loop (HIL) decisions may vary based on the scope and risk profile. In some cases, HIL requirements may be minimal or even unnecessary if the risk and impact are low, or if development of an AI initiative is still in its early stages.
- Some artefacts may take the form of either a Strategy, a Plan, or both, depending on AI system maturity and scale.
- Product- or system-level elements such as the AI Assurance Plan and AI Product Management Plan are stage gated, and their implementation should align with the maturity and intended application of the AI-enabled service.
- These scope levels also align with the proportional application of the Readiness Assessment Framework as visualised through the spider diagram (Figure 3). For example, low organisational readiness combined with a high-risk use case would trigger higher governance requirements, ensuring safeguards keep pace with the intended application.

Ensuring the framework reflects the operational realities and organisational responsibilities will require validation of the components with representative stakeholders, such as IT governance and data governance representatives. Descriptions of each artefact are provided in Appendix A: Description of AI governance artefacts, and descriptions of accountabilities are in Appendix B: Roles, responsibilities and accountabilities.

5 Summary and Recommendations

The AI Readiness Assessment Framework provides a systematic set of tools for assessing preparedness across four core domains of Strategy, Organisation, Data, and Technology, ensuring readiness for next-stage investment and deployment. This framework recognises that AI readiness extends beyond technology. The framework includes:

- A multi-domain Venn diagram showing how the domains overlap to contribute to AI readiness.
- A set of criteria for each domain, with recommendations for which AI lifecycle stages the criteria should be assessed.
- A spider diagram that can help an organisation visualise how prepared they are, relative to a reference AI-readiness profile, and where investment and effort should be focused as a priority to uplift readiness before progressing onto subsequent stages.

In preparation for an AI-enabled service, it is recommended that an organisation:

- Conduct an AI readiness assessment to validate current state and identify which of the Strategy, Organisation, Data, and Technology domains require uplift before progressing the technological capabilities of the AI-enabled service.
- Use the AI Readiness Assessment Framework to baseline current capabilities and sequence delivery of the AI-enabled service, supported by targeted improvements in the Strategy, Organisation, Data, and Technology domains.
- Consider embedding this framework into AI governance functions and consider it for integration into the organisation's approval process for AI initiatives.

The AI governance structure should be positioned to align, and where appropriate, overlap with organisation IT and data governance functions, while also maintaining alignment with enterprise policies. This integrated approach ensures:

- Consistency with established data governance practices.
- Compliance with government or organisation-wide AI and digital policies.
- Coordination with existing risk management frameworks.
- Integration with security and privacy protocols.

Organisational-wide AI governance and artefacts should be developed during the early stages of the AI lifecycle when risk and governance burden is low. This sets the foundations for more detailed system-level or product-level governance that can be implemented with greater agility as the system matures.

In preparation for an AI-enabled service, it is recommended that an organisation:

- Define the scope and risk profile of the AI-enabled service and adopt governance artefacts and accountabilities based on system complexity and risk profile.
- Establish the AI governance function early in the lifecycle of the AI-enabled.
- Implement foundational governance artefacts early and at the appropriate level for the current low-risk development stage (including an AI Strategy, Accountability Framework, and an AI Governance Framework that aligns with the data governance framework).

This tiered governance approach operationalises the AI readiness profiles across the AI lifecycle, as outlined earlier, turning abstract maturity levels into specific accountabilities, plans, and artefacts.

In summary, this white paper introduces practical tools to support organisational readiness for AI-enabled service delivery. It also underscores the importance of a balanced, governance-driven approach to AI adoption, ensuring that organisations are not only technically prepared but also strategically, organisationally, and ethically ready to harness the transformative power of AI.

Appendix A: Description of AI governance artefacts

AI strategy: An organisational-level AI strategy to implement AI policies and processes. The AI Strategy should also describe what successful culture and values look like at the departmental and divisional level, for the use and/or development of AI systems as an enabler to achieve the organisation's business priorities.

Risk and impact management plan: Establishment of AI specific risk management arrangement to think critically about context and potential or unexpected negative and positive impacts, and actions to mitigate these risks. Relevant references include the Queensland Government's FAIRA[11], and NIST AI Risk Management Framework[12].

Monitoring and continuous improvement plan: Plans, measures and metrics for continuous or routing monitoring of the AI-enabled service to ensure it performs as intended, and that its model and outputs are acceptable. Relevant references include the GAO-21-519SP.

AI product strategy: Product strategy for the AI-enabled service.

Change management strategy: To ensure business readiness for AI systems, and to ensure that data culture is aligned with AI system delivery. Major change management process to align with data strategy and instil culture of AI readiness. Inclusion of change management strategy. Potential for transformation of the way foundational data is handled.

Security and privacy compliance framework: Framework to ensure the AI-enabled service complies with all relevant security and privacy policies and arrangements, as mandated by Government regulators, and/or corporate and IT governance.

Regulatory / legal framework: Framework to ensure that the AI-enabled service complies with all relevant regulatory and legislative requirements, as mandated by Government regulators, and/or corporate and IT governance.

Data ethics strategy: Strategy that describes the use of data-enabled AI and AI-enabled data discovery in a fair and accessible manner.

Data assurance and integrity strategy: Strategy that describes the use of data-enabled AI and AI-enabled data discovery in a trustworthy, transparent, traceable, and explainable manner.

Contestability and human oversight framework: A structured approach to ensure that outputs or decisions made by the AI-enabled service can be challenged or contested, especially when they significantly impact individuals or groups; as well as ensuring human-in-the-loop and human accountability is maintained throughout the AI-enabled service's lifecycle.

AI assurance plan: Outlines processes and practices required to ensure the AI-enabled service consistently aligns with the strategic goals and governance framework established by the organisation or government agency. It provides an objective and independent mechanism for monitoring alignment between the AI strategy and implementation.

[11] Queensland Government FAIRA Framework. www.forgov.qld.gov.au/information-and-communication-technology/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/faira-framework.

[12] NIST, 2024. AI Risk Management Framework. www.nist.gov/itl/ai-risk-management-framework.

Appendix B: Roles, responsibilities and accountabilities

Governance roles and responsibilities (presented in Table 3) are guided by the functions and artefacts required within the AI Governance Structure.

Table 3: Governance roles and responsibilities.

Role	Responsibility / Function
Accountable Official	Designated accountable official at the organisation/agency for the responsible use of AI. This may be an additional responsibility for the Chief Information Officer / Chief Data Officer.
AI Executive Steering Group	Senior governance body at the organisational level to provide coordination and oversight of AI policies and activities. The AI Executive Steering Group has oversight of the various subcommittees, working groups, or officers who are responsible for providing practical guidance on area-specific implementation of AI strategy.
AI Strategy Officer	A custodian or stewardship role specifically tasked with monitoring alignment between the AI strategy and practical implementation of the Governance Framework, ensuring that all domain functions meet strategic goals. The custodian would be responsible for day-to-day governance and compliance requirements. This is an independent and objective function that reports to the AI Executive Steering Group, ensuring that AI assurance remains unbiased. The function may also be responsible for identifying conditions, if any, under which the AI system may be scaled or expanded beyond its current use. Additionally, the function would ensure connection with rapidly evolving AI technologies and regulatory landscape to ensure the business maintains relevance.
AI Data Governance Officer	A specialist custodian role responsible for ensuring data governance processes evolve to meet the unique demands of AI implementation. This role would oversee the preparation and maintenance of AI-ready datasets, aligning data practices with emerging AI requirements, such as metadata standards and ethical data handling for AI systems. The role bridges operational data governance with AI governance, and may require a role adaptation or an entirely new position, depending on the demand for new AI-ready data requiring support. The role may also be responsible for coordinating with the AI Strategy Officer to ensure consistency and readiness across AI-enabled initiatives.
AI Safety and Assurance Officer	A dedicated function responsible for overseeing the safe design, deployment, and ongoing monitoring of AI model architectures and associated data governance practices. This role ensures that AI-enabled systems align with best practices for safe, secure, and ethical operation. It bridges technical safety (e.g. model robustness and reliability) with governance responsibilities. This role would work closely with the AI Data Governance Officer, Risk and Impact Management, and Monitoring and Continuous Improvement functions, while serving as a technical advisor to the AI Executive Steering Group in AI model safety concerns.
Data Ethics Subcommittee / Working Group	Comprising multidisciplinary stakeholders, including internal stakeholders alongside external stakeholders who would use or be impacted by the service. The committee is responsible for providing practical guidance on how to apply the ethical principles for AI to the different phases of the life cycle of the AI-enabled service.
Security and Privacy Subcommittee / Working Group / Officer	An individual or group that assesses and ensures compliance with and implementation of data security and privacy controls within the AI Governance Framework. This role may somewhat or significantly overlap with an equivalent role within the organisation's data governance framework.

Role	Responsibility / Function
Risk and Impact Management Subcommittee / Working Group / Officer	Existing organisational risk management pertaining to Data Governance may be insufficient when adapted to AI systems. Within the AI Governance framework, Risk and Impact Management would be established as a cross-functional capacity specifically aimed at introducing processes that better support the identification, analysis and mitigation of AI risks, including to users, systems, and interconnectivities and dependencies of data streams that operationalise the AI-enabled service.
Monitoring and Continuous Improvement Subcommittee / Working Group / Officer	This function is an internal auditor role that develops and oversees plans for continuous monitoring of the AI-enabled service to ensure it performs as intended, and helps track AI risks. The role entails setting up metrics for secure and trustworthy AI, monitoring AI systems outputs and interactions, and identifying and mitigating any threats. Depending on the scale of AI adoption, development and risk profile, this function may overlap with or initially be a part of the Risk and Impact Management function.
Regulatory and Legal Working Group / Officer	An individual or group that assesses and ensures implementation of legislative and regulatory controls within the AI Governance Framework. This role may somewhat or significantly overlap with an equivalent role within the organisation's data governance framework.
Human Oversight function	Assess and ensure human oversight in terms of AI system monitoring, decision making, as well as mitigation of risks or issues raised by users with regards to correctness, quality, accuracy, reliability, usefulness of the AI-enabled service's outputs.
Application Manager/s	A technical system or product owner that has responsibilities that align with the specific areas such as ensuring system compliance, data integrity, or technical performance, and would be responsible for operationalising and maintaining systems according to the subcommittees' guidelines and decision frameworks. Note this role has not been explicitly outlined in Figure 7 or Figure 8, however it is a critical governance role that sits under or within many of the area-specific subcommittees or working groups (e.g. data integrity, security and privacy, monitoring).
AI Standards Committee / Working Group	A function that: i) establishes and shares best practices for AI governance; ii) provides frameworks and guidelines for key technology areas such as foundational models, GenAI, Large Language Models, AI agents, etc; iii) standardises terminology, data formats, and interfaces to facilitate the integration of AI systems with the organisation's existing data infrastructure. This function may overlap with the Data Managers group and Data Standards Committee within the data governance framework.

The chain of accountability of these roles is presented Figure 7and Figure 8. Two representative options are provided:

Option 1

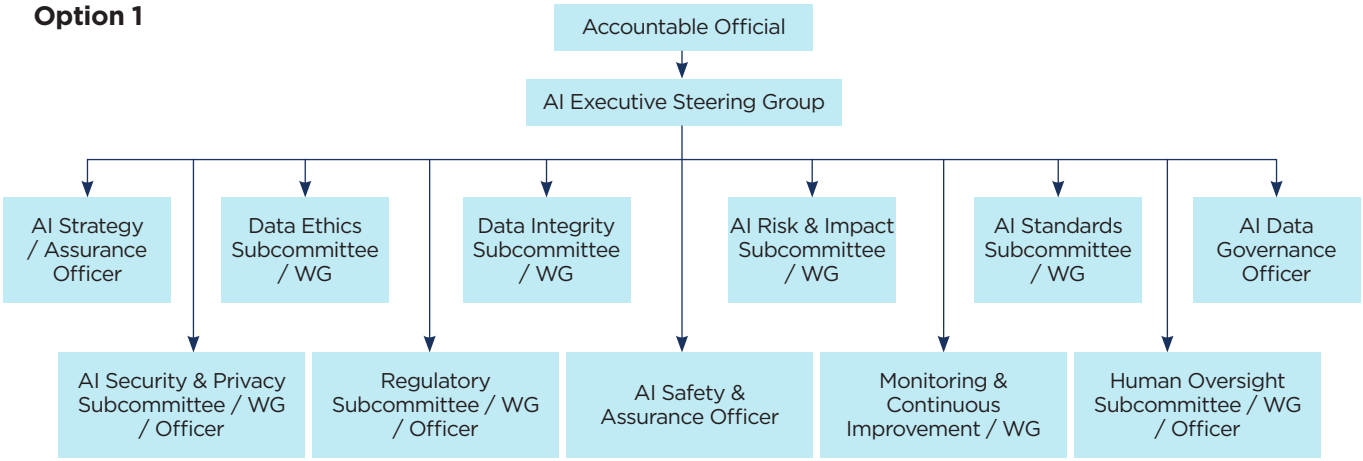


Figure 7: Chain of accountability option 1.

Option 2

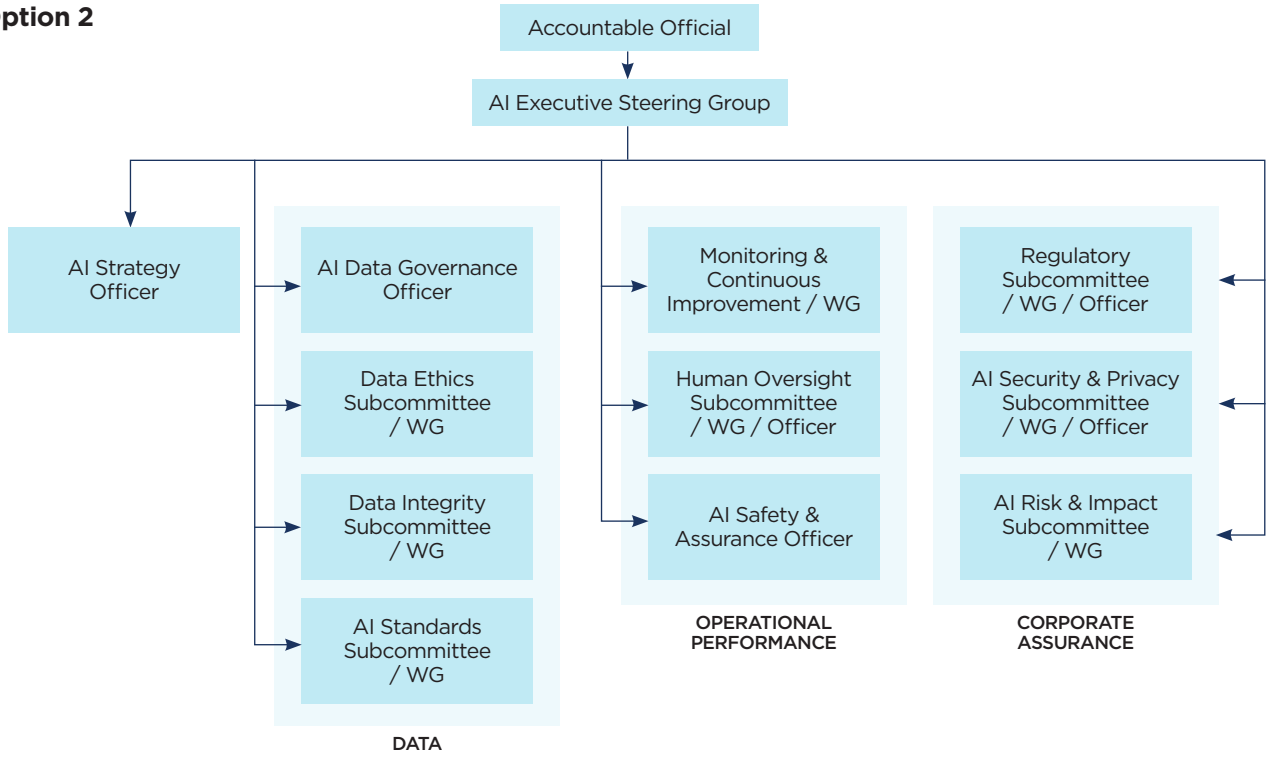


Figure 8: Chain of accountability option 2.

Appendix C: Assessment criteria

C.1 AI-Readiness Domain: Strategy

Strategy, Governance, and Accountability underpin the responsible and strategic adoption of AI. This domain ensures AI use is led from the top, aligned with organisational, enterprise, and broader corporate priorities. AI adoption is governed through a clear strategy and guided by appropriate governance frameworks that align with ICT governance and public sector legislation. The Governance Framework, functions, and artefacts should be fit-for-purpose, and implemented proportionally to the scale, complexity, risk profile, and lifecycle of the AI-enabled service. This domain answers the question: *"How are we doing this, and how are we ensuring it is done responsibly?"*

Table 4 outlines AI-readiness criteria for the Strategy domain, as well as associated responsible roles for each category.

Table 4: AI-readiness categories, criteria, and responsibilities for the Strategy domain.

Strategy Categories	Criteria	AI Lifecycle Stages	MoSCoW Prioritisation	Examples of Measures
AI Strategy	An organisational AI Strategy has been endorsed by relevant delegates.	1, 2	Must – Essential for alignment, governance, accountability	• Endorsement of AI Strategy by leadership • Established frequency of cross-functional alignment sessions on AI Strategy
AI Governance	A **fit-for-purpose AI Governance Framework** is established and actively managed, proportionate to the scale, complexity, risk profile, and lifecycle of the AI-enabled service. The framework is informed by a maturity model to ensure appropriate governance measures are applied at each stage of design, development, operationalisation, and closeout.	1, 2, 3	Must – Non-negotiable for accountability and oversight across all stages, but critical at early stages	• Alignment of AI governance with ICT governance • Documented governance controls meet requirements of AI policies • Maturity model established to guide future state attributes and outcomes of AI-enabled service
Data Governance	Data governance framework is established and actively managed.	1, 2, 3	Must – Essential for ensuring AI quality, fairness, security	• Data governance framework is endorsed and version-controlled • % of data governance processes with active ownership and lifecycle status

Strategy Categories	Criteria	AI Lifecycle Stages	MoSCoW Prioritisation	Examples of Measures
Regulatory and Legislative	Regulatory, legislative, and legal considerations are aligned with those of the relevant department (e.g. responsible for enterprise architecture) and addressed.	1, 2, 3	Must – Required for legal compliance and organisational integrity for all stages, but critical for early stages.	• Assessments in place to evaluate compliance with regulation and legislation
Risk and Impact Management	**Risk and impact management plan** has been prepared and is actively managed. Risk frameworks, methods and processes are in place based on best-practice risk management frameworks including AI.	1 to 4	Must – Foundational for AI assurance	• Percentage completion and alignment with selected risk assessment (against defined thresholds) • Mitigation plan established to address identified risks
	Relevant risk assessments have been conducted, reviewed with relevant delegates, and signed off by the relevant authorised delegates.		Must – Essential for securing approvals to proceed	
Human, Societal, and Environmental Wellbeing	**AI public value, risk, impact plan** is established and actively managed, and is proportionate to the scale, complexity, risk profile, and lifecycle of the AI-enabled service. The framework is informed by a maturity model to ensure appropriate governance measures are applied at each stage of design, development, operationalisation, and closeout. For government implementation, it complies with appropriate policies.	1 to 4	Must – Essential for public-facing AI initiatives	• Maturity model established to guide future state attributes and outcomes of AI-enabled service • Assessments in place to evaluate compliance with public sector ethics and inclusion policies
Human-Centered Values	**Human-centred design and use policy** is established and actively managed, and is proportionate to the scale, complexity, risk profile, and lifecycle of the AI-enabled service. The framework is informed by a maturity model to ensure appropriate governance measures are applied at each stage of design, development, operationalisation, and closeout. It complies with appropriate human rights and impacts policies.	2, 3	Must – Important for ethical AI. Foundations are laid upfront, and implemented during later stages	• Maturity model established to guide future state attributes and outcomes of AI-enabled service • Assessments in place to evaluate compliance with human rights policies and alignment with human-centred design

Strategy Categories	Criteria	AI Lifecycle Stages	MoSCoW Prioritisation	Examples of Measures
Fairness	**AI fairness strategy** (modelling, processes, outcomes, accessibility) is established and actively managed, and proportionate to the scale, complexity, risk profile, and lifecycle of the AI-enabled service. The framework is informed by a maturity model to ensure appropriate governance measures are applied at each stage of design, development, operationalisation, and closeout.	2, 3, 3	Must – Important for public-facing AI initiatives	• Maturity model established to guide future state attributes and outcomes of AI-enabled service. • Audits in place to evaluate bias and accessibility risks
Privacy Protection and Security	**Privacy protection and security compliance plan** is established and actively managed, and is proportionate to the scale, complexity, risk profile, and lifecycle of the AI-enabled service. The framework is informed by a maturity model to ensure appropriate governance measures are applied at each stage of design, development, operationalisation, and closeout. It complies with relevant information privacy policy and legislation.	1 to 3	Must – Essential for compliance	• Audits in place to assess privacy compliance for the AI-enabled service use case • Defined roles and responsibilities to assign and control access to information
Reliability and Safety	**Monitoring and continuous improvement plan** is established and actively managed, and is proportionate to the scale, complexity, risk profile, and lifecycle of the AI-enabled service.	4, 5, 6	Must – Essential for compliance across lifecycle, but critical to establish at early stages	• Test plans in place for system availability and recovery • Benefits realisation plan established and monitored
	Service measurement and reporting, benefits realisation, service review and improvement processes in place.		Should – Important, may be developed over AI-enabled service lifecycle	

Strategy Categories	Criteria	AI Lifecycle Stages	MoSCoW Prioritisation	Examples of Measures
Transparency and Explainability	**AI assurance management plan** is established and actively managed, and is proportionate to the scale, complexity, risk profile, and lifecycle of the AI-enabled service.	1, 2, 3, 4	Must – Enables trust and auditability across entire lifecycle, but critical at early stages	• AI assurance framework in place with endorsement • Public availability of responsible disclosure notices • Assurance reviews are conducted per AI lifecycle stage
	Data assurance and integrity strategy is established and actively managed, and is proportionate to the scale, complexity, risk profile, and lifecycle of the AI-enabled service.		Must – Enables trust and auditability across entire lifecycle, but critical at early stages	
	Preparation of a transparent and responsible disclosure so people can understand when they are being significantly impacted by AI, and can clearly identify when an AI system is engaging with them.		Could (Important in mature stages, less relevant early)	
	AI assurance management plan, and data assurance and integrity strategy, complies with appropriate public records policies and metadata management principles.		Must – Essential for compliance, when the management plan is established	
Delivery	The AI lifecycle stages utilised follow those established by the Australian Cyber Security Centre.		Must – Essential for ensuring AI implementations are appropriately staged	• Nomination of project delivery stage in project artefacts
Contestability	**Contestability and human oversight plan** is established and actively managed, and is proportionate to the scale, complexity, risk profile, and lifecycle of the AI-enabled service. The framework is informed by a maturity model to ensure appropriate governance measures are applied at each stage of design, development, operationalisation, and closeout.	4, 5, 6	Must – Important in mature stages, less relevant early, or less relevant when human input is minimal	• Human oversight roles designated for critical AI decisions • Processes established to handle contestations, user feedback, and escalations
Accountability	An **accountability framework** is established and actively managed, and complies with appropriate financial and governance accountability policies and standards.	1, 2	Must – Essential for compliance	• Assessments in place to evaluate compliance with appropriate policies and requirements • Responsible officers are assigned across functions and lifecycle stages of the AI-enabled service
	Line of sight is established for accountability, and Responsible Officers have been designated.		Must – Essential for accountability and responsibility	

C.1 AI-Readiness Domain: Organisation

The Organisation domain focuses on the leadership, workforce, organisational capability, and cultural readiness required to deliver, sustain and scale the AI-enabled service. Leadership plays a key role in aligning the direction of AI initiatives with the organisation's long-term priorities and strategies, including socialising the use case, benefits, and investment justification. Organisational readiness is facilitated by stakeholder and change management, and enabled by workforce, business, and delivery capabilities, and cultural readiness to implement. This domain answers the questions: *"What is the problem we are solving, who are we solving this for, and who will deliver this?"*

Table 5 outlines AI-readiness criteria for the Organisation domain.

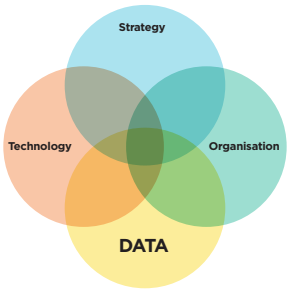
Table 5: AI-readiness categories and criteria for the Organisation domain.

Organisation Categories	Criteria	AI Lifecycle Stages	MoSCoW Prioritisation	Examples of Measures
Stakeholder Management	Stakeholder management established. This includes: • Stakeholders identified and processes in place to proactively manage expectations. • Community of practice (of users) or a reference group (of experts) established.	1 to 6	Must – Engagement essential to build trust, secure involvement	• Establishment of stakeholder register and engagement plan • Stakeholder feedback incorporated into decisions made by community of practice or reference groups
Change Management	Change and communication management plan is established and actively managed, and is proportionate to the scale, complexity, risk profile, and lifecycle of the AI-enabled service. GenAI service onboarding and transition processes established and actively managed, including user support and training processes, access management, incident management, and problem management.	1, 2, 3	Must – Stakeholder and user transition, support, and cultural readiness across lifecycle, but critical in early stages	• Change management plan documented and version-controlled • % of personnel receiving onboarding sessions and training
Talent, resourcing	Workforce planning is in place to ensure appropriate skills and capacity to support the AI-enabled service, appropriate to the scale, complexity, risk profile, and its lifecycle. This includes: • Required skills are identified (technical, ethical, operational). • Capability uplift or recruitment strategies are in place. • Training and professional development plans are considered. • Developer ecosystem is in place to design, develop, test, and implement the tool / service.	1, 2, 3, 4	Must – Ensure skills and capacity strategies are in place to support lifecycle stages, but critical in early stages	• Skills gap analysis undertaken and documented • Recruitment and/or upskilling initiatives launched

Organisation Categories	Criteria	AI Lifecycle Stages	MoSCoW Prioritisation	Examples of Measures
Business capacity	Organisation/department confirms capacity to support the AI-enabled service throughout its lifecycle.	2, 3, 4	Must – Organisational capacity continuity planning essential to support lifecycle stages	• Roles and responsibilities are defined and resourced • Business continuity and risk mitigation plans are established • Business support processes documented (against agreed threshold)
Delivery Capability	Delivery capability is in place to design, develop, test and implement the AI-enabled service, including program and project delivery approaches, cross-functional delivery teams where appropriate, milestone and dependency planning.	1 to 3	Must – Resources are available to execute plans and to deliver	• Delivery approach defined, documented and endorsed • Formation of cross-functional teams for delivery • Number of milestones (against agreed threshold) tracked against delivery roadmap
Finance and cost management	Financial management processes are in place to plan, maintain and execute the GenAI business service. This includes budgeting, costing, pricing (revenue), link to Service Level Agreement, reporting, and cost benefit analysis. Governance in place to ensure technology investments meet business needs.	1, 2, 3	Must – Prerequisite for informed decision-making and long-term viability; critical in early stages	• Approval of cost-benefits analysis • Budget allocated and tracked for AI-enabled service
Use case / Business Case	Business case for the AI-enabled service confirms the following: • Has a clearly specified purpose, value and objectives for the new GenAI offering. • Demonstrates strategic alignment with organisation and departmental priorities. • Investment logic is clearly articulated, including problem statement and positive impact generated through development and delivery. • Associated benefits are defined alongside practical outcomes and metrics. • Key features are specified.	1, 2	Must – Essential for defining the purpose and value of the AI-enabled service in the first instance	• Business case endorsed by appropriate authoritative delegate • KPIs defined against business case • Assessment in place to evaluate compliance with organisational/ departmental investment framework requirements

Organisation Categories	Criteria	AI Lifecycle Stages	MoSCoW Prioritisation	Examples of Measures
Cultural Readiness	Strategies for workforce planning are aligned with long-term AI Strategy. There is shared ownership of the challenges, accountabilities across departments and business units.	1 to 4	Must – Essential in early stages and matures over time with stakeholder engagement and change management	• Establishment of cross-functional or cross-unit AI working groups • Number of units represented in planning or ownership roles (against agreed threshold)
Governance Framework	As per the Strategic domain, fit-for-purpose ICT, data and AI governance frameworks are established and applying appropriate governance measures are applied at each stage of design, development, operationalisation, and closeout.	1 to 6	Must – Non-negotiable for accountability and oversight across all stages, but critical at early stages	As per the Strategic domain: • Alignment of AI governance with ICT governance • Documented governance controls meet requirements of AI policies • Maturity model established to guide future state attributes and outcomes of AI-enabled service
Digital Literacy	Pathways to organisational and digital literacy is supported, alongside business ability to adopt emerging and evolving AI technologies.	4, 5, 6	Must – Supports AI-enabled service adoption	• Digital literacy initiatives or training established and completed • % of workforce trained in GenAI fundamentals and data ethics
Executive Leadership	Leadership is committed and works to align GenAI use case with overall strategy.	1, 2	Must – Essential for sponsorship and strategic alignment across lifecycle; critical in early stages	• Executive Sponsor or Accountable Officer identified and active • % of executive reports from senior departmental/ organisational management referencing the AI-enabled service

C.1 AI-Readiness Domain: Data



The Data domain focuses on the availability, accessibility, quality, security, and governance of data, and the need to train, validate, and operationalise the AI-enabled service. It aligns technological capability and agility with business needs, enabling integration into the broader organisational context. This domain assesses the readiness of the AI data with trust, traceability, and integrity in mind as the AI-enabled service matures through its lifecycle. This domain answers the question: *"What is the data that is foundational to technology adoption?"* The criteria and metrics have been adapted from the Australian Cyber Security Centre's Cybersecurity Information Sheet for AI Data Security[13].

Table 6 outlines AI-readiness criteria for the Data domain.

Table 6: AI-readiness categories and criteria for the Data domain.

Data Categories	Criteria	AI Lifecycle Stages	MoSCoW Prioritisation	Examples of Measures
AI Data	AI data completeness, quality, accuracy, availability, and assurance processes are established and actively managed. This includes • Data classification completed with appropriate access controls	1, 2, 3	Must – Foundational for AI success	• % of datasets with no missing values for mandatory fields (against defined threshold) • % of datasets used for AI training that pass QA/QC rules (against defined threshold) • Data quality assessments conducted and signed off
Tracking AI Data Provenance	Processes for sourcing reliable data and managing data provenance are established and routinely applied. AI data inputs are sourced from trusted origins, with provenance tracked and verified through established governance processes.	1, 2	Must – Foundational for traceability	• Evidence of data logging across the AI data lifecycle • Evidence of a provenance database • Provenance planning and auditing upfront and implemented during data ingestion
AI Data Integrity	Mechanisms are in place to verify and maintain the integrity of AI-related data throughout its lifecycle, including storage and transport between systems.	2, 3, 4, 5	Must – In place for integrity across all stages; critical in early-mid stages to establish	• Evidence of integrity verification such as checksums, hashing, or through automated processes for continuous verification and audit
Trust and modelling	Controls are in place to detect and mitigate risks of maliciously-modified data, bias, data poisoning, data drift.	3, 4, 5	Must – for trusted and secure modelling; critical in mid stages during build and testing	• Mechanisms for bias detection implemented in training data • Checks for data drift at established intervals during productionisation

[13] Australian Cyber Security Centre AI Data Security. www.cyber.gov.au/resources-business-and-government/governance-and-user-education/artificial-intelligence/ai-data-security.

Data Categories	Criteria	AI Lifecycle Stages	MoSCoW Prioritisation	Examples of Measures
AI data quality	Processes are established to manage assess and correct for risks around imperfect data, such as errors, noise, outliers, gaps.	2	Should – Reduce noise and mistakes	• Data quality dimensions tracked (e.g. completeness, quality, accuracy) • Boundaries defined for acceptable noise, outliers, or incompleteness
AI data verification	Following on from AI data provenance tracking, processes for data verification are in place to authenticate and track revisions or modifications of data	3, 4	Should – Useful for traceability	• Use of digital signatures or equivalent verifiable methods, or credentialling
AI data access and authorisation	Processes for data access and authorisation are implemented to restrict unauthorised data access, or to control use.	2, 3	Must – Critical for compliance, access control, use case alignment	• Verification of data sensitivity and required protection measures established • Comprehensive security testing, adversarial testing plans established
AI data storage	AI data is stored in secure environments and storage devices with the appropriate cyber-physical protections.	3, 4, 5, 6	Must – Key for securing data	• Use of secure environments • Alignment with relevant ISO standards • Establishment of incident reporting metrics
AI data architecture	Provisions have been made for secure environments for the protection of sensitive data, and to maintain data integrity during processing.	1, 2, 3	Must – Foundational for guiding design and development decisions, and for future scalability	• Demonstrated compliance with industry standards for security such as NIST FIPS 140-2[14]
AI data encryption	Encryption protocols are in place to protect sensitive AI data at rest, in transit, and during processing.	2, 3, 4	Must – for securing sensitive datasets	• Demonstrated compliance with industry standards for encryption
AI data privacy	Privacy-preserving techniques are applied to AI data and applied consistently.	3, 4, 5, 6	Must – critical for public-facing applications	• Evidence of techniques including data depersonalisation, differential privacy, decentralised learning.

[14] National Institute of Standards and Technology. NIST FIPS 140-2 Security Requirements for Cryptographic Modules. https://csrc.nist.gov/pubs/fips/140-2/upd2/final.

Data Categories	Criteria	AI Lifecycle Stages	MoSCoW Prioritisation	Examples of Measures
AI data deletion	Protocols of managing or disposing of end-of-life data, data that is no longer fit-for-purpose, or data that is not needed from all storage locations.	6	Should – Important for lifecycle governance, though not urgent upfront	• Evidence that data is disposed of securely using approved methods that prevent recovery or unauthorised access.
AI data security risk assessments	Processes to conduct AI data security risk assessments are established to monitor, identify, and mitigate risks during the AI life cycle.	1 to 6	Must – Essential for assurance and compliance	• Evidence of adherence to industry standard AI risk management frameworks such as NIST SP800-3r2[15] or the NIST AI RM[16].

C.1 AI-Readiness Domain: Technology

The Technology domain focuses on the digital, infrastructure, and AI technological capabilities required to deliver the AI-enabled service. It aligns technological capability and agility with business needs, enabling integration into the broader organisational context. This domain assesses the readiness of the AI models and enabling infrastructure, with scalability, reuse, and integration in mind as the tool matures through its lifecycle. This domain answers the question: *"What are we going to do it with?"*

Table 7 outlines AI-readiness criteria for the Technology domain.

Table 7: AI-readiness categories and criteria for the Technology domain.

Tecnology Categories	Criteria	AI Lifecycle Stages	MoSCoW Prioritisation	Examples of Measures
Technology agility throughout lifecycle development	Processes are in place to guide development of the AI-enabled service. This includes: • Assessment of technical feasibility. • Documentation of solution architecture and technical architecture. • Design and development processes are user-informed and iterative. • Design is modular to support both infrastructure and GenAI tool scalability. • Structures to stage-gate development towards operationalisation.	1 to 6	Must – Essential to ensure scalable, user-informed solutions	• Documented and endorsed technical and solution architecture • Documented design and development cycle involving user feedback
GenAI Product Strategy	GenAI business service strategy defined, including an understanding of its performance, demand, and potential future state of the service (feature roadmap).	2, 3, 4	Must – Strategy informs design and development	• AI-enabled service service strategy in place and endorsed • Plan for evaluation of performance against strategy in place

[15] National Institute of Standards and Technology. NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[16] National Institute of Standards and Technology. NIST AI Risk Management Framework. www.nist.gov/itl/ai-risk-management-framework.

Tecnology Categories	Criteria	AI Lifecycle Stages	MoSCoW Prioritisation	Examples of Measures
AI Model	Model selection, development, and deployment processes are established and actively managed. This includes: • Model validation for performance, accuracy, and alignment with use case. • Model testing and evaluation follows best practice and is documented and repeatable. • Bias, fairness, and explainability have been considered. • Model monitoring mechanisms are defined for performance drift and retraining where needed.	3, 4, 5, 6	Must – Core to delivery of the AI-enabled service	• Evidence of AI model/s undergoing regular testing and drift monitoring • % accuracy of model validation against use case or against trusted reference results
Infrastructure Management and Deployment	Infrastructure (e.g. on-prem or cloud or hybrid) is fit-for-purpose, scalable, and aligned with enterprise architecture. This includes: • Ability and availability of computing, data storage, networking resources to support AI development and deployment. • Technical and operational responsibilities for infrastructure are clearly identified and assigned. • Infrastructure can be re-used or shared with other programs or AI initiatives.	2, 3, 5	Must – Needed to support data storage and AI model delivery	• Infrastructure is available to support AI development and deployment as required • % of infrastructure reused or shared across other programs or AI initiatives
AI-enabled service / service scalability	The AI-enabled service or service is designed for scalability across functions and users. This includes: • Supported scaling of architecture. • Plans for growth, re-use of infrastructure, integration across business units, for example integration with the existing data services and portals. • Scaling of the AI-enabled service is structured by a maturity model, with defined attributes and outcomes at each level of maturity.	2 to 5	Should – Important for planning, though scaling becomes critical only later	• Documented maturity model to guide future state attribute and outcomes of the AI-enabled service • % of infrastructure reused or shared across other programs or AI initiatives

Tecnology Categories	Criteria	AI Lifecycle Stages	MoSCoW Prioritisation	Examples of Measures
User-centric development	To ensure validation of the selected technology: • Design and development processes are user-informed and iterative (responsiveness). • Business needs are validated (relevance).	2, 5, 6	Should – Integrated early, progressively strengthened over iterations and lifecycle maturity	• User satisfaction / user feedback on AI-enabled service usability • Evidence of user or stakeholder feedback integrated into development or into updates
GenAI Product Management	GenAI business service is designed including: • Service design, detailed service management, planning and structure, customer interaction points defined and processes. • Established performance benchmarks and service level agreements. • Established service catalogue, service levels defined. Including specifications for service continuity, information security, supplier management, capacity and availability.	4, 5, 6	Could – Important for early planning, though support and service; becomes critical towards productionisation	• Established intervals of service performance reviews • Evidence of customer interaction points mapped (e.g. journey maps) • Evidence of customer interaction points incorporated into AI-enabled service (e.g. feature audit / usability feedback)

Appendix D: Relevant AI policies, frameworks and reference documents

The following curated bibliography provides additional reading and context to the GSQ report that this whitepaper was drawn from.

1. Digital Transformation Agency, 2021, *Policy for the responsible use of AI in government*, viewed 28 October 2023, www.digital.gov.au/policy/ai/policy.
2. Springer, 2022, *Defining organizational AI governance*, viewed 28 October 2023, https://link.springer.com/article/10.1007/s43681-022-00143-x.
3. Queensland Government, 2021, *FAIRA Framework*, viewed 28 October 2023, www.forgov.qld.gov.au/information-and-communication-technology/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/faira-framework.
4. Australian Cyber Security Centre, 2023, *AI Data Security*, viewed 28 October 2023, www.cyber.gov.au/resources-business-and-government/governance-and-user-education/artificial-intelligence/ai-data-security.
5. Queensland Government, 2021, *Foundational artificial intelligence risk assessment framework*, viewed 28 October 2023, www.forgov.qld.gov.au/information-technology/queensland-government-enterprise-architecture-qgea/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/faira-framework.
6. AWS, 2023, *Securing generative AI: An introduction to the Generative AI Security Scoping Matrix*, viewed 28 October 2023, https://aws.amazon.com/blogs/security/securing-generative-ai-an-introduction-to-the-generative-ai-security-scoping-matrix/.
7. Gartner, 2025, *AI Maturity Model & Roadmap Toolkit*, viewed 28 October 2023, www.gartner.com/en/chief-information-officer/research/ai-maturity-model-toolkit.
8. Australian Cyber Security Centre, 2023, *AI Data Security*, viewed 28 October 2023, www.cyber.gov.au/resources-business-and-government/governance-and-user-education/artificial-intelligence/ai-data-security.
9. ProductPlan, n.d., *MoSCoW Prioritization: A prioritisation technique for managing project scope*, viewed 28 October 2023, www.productplan.com/glossary/moscow-prioritization/.
10. Queensland Government, 2022, *Public Sector Act 2002*, viewed 28 October 2023, www.legislation.qld.gov.au/view/whole/html/inforce/current/act-2022-034.
11. Queensland Government, 1994, *Public Sector Ethics Act 1994*, viewed 28 October 2023, www.legislation.qld.gov.au/view/pdf/2014-07-01/act-1994-067.
12. Queensland Government, 2011, *Work Health and Safety Act 2011*, viewed 28 October 2023, www.legislation.qld.gov.au/view/html/inforce/current/act-2011-018.
13. Accenture, 2022, *Climate Action Plan 2020-2030*, viewed 28 October 2023, https://assets.nationbuilder.com/queenslandconservation/pages/5382/attachments/original/1659490046/Queensland_Climate_Action_Plan-FINAL-1_August-PDF-FINAL_Embargoed_for_release_2_Aug.pdf.
14. Queensland Government, 2021, *Inclusion and Diversity Strategy 2021-2025*, viewed 28 October 2023, www.forgov.qld.gov.au/__data/assets/pdf_file/0022/184144/queensland-public-sector-inclusion-and-diversity-strategy-2021-2025.pdf.
15. Queensland Government, 2009, *Integrity Act 2009*, viewed 28 October 2023, www.legislation.qld.gov.au/view/pdf/current/act-2009-052.
16. Queensland Government, 1994, *Environmental Protection Act 1994*, viewed 28 October 2023, www.legislation.qld.gov.au/view/html/inforce/current/act-1994-062.
17. Queensland Government, 2022, *Government Artificial Intelligence Governance Policy*, viewed 28 October 2023, www.forgov.qld.gov.au/information-technology/queensland-government-enterprise-architecture-qgea/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/artificial-intelligence-governance-policy.
18. Queensland Government, 2019, *Human Rights Act 2019*, viewed 28 October 2023, www.legislation.qld.gov.au/view/html/inforce/current/act-2019-005.

19. Queensland Government, 2020, *Human Rights Resources*, viewed 28 October 2023, www.forgov.qld.gov.au/service-design-and-delivery/deliver-public-services/comply-with-the-human-rights-act/human-rights-resources.

20. Queensland Government, 2021, *Proactive Protection of Vulnerable Persons*, viewed 28 October 2023, www.forgov.qld.gov.au/__data/assets/pdf_file/0025/184048/faqs-proactive-protection-vulnerable-persons.pdf.

21. Queensland Government, 2021, *Artificial Intelligence and public records*, viewed 28 October 2023, www.forgov.qld.gov.au/information-technology/recordkeeping-and-information-management/recordkeeping/resources-and-tools-for-records-management/artificial-intelligence-and-public-records.

22. Australian Government, 1988, *Privacy Act 1988*, viewed 28 October 2023, www.legislation.gov.au/C2004A03712/2019-08-13/text.

23. Queensland Government, 2021, I*nformation security classification framework (QGISCF)*, viewed 28 October 2023, www.forgov.qld.gov.au/information-technology/queensland-government-enterprise-architecture-qgea/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/information-security-classification-framework-qgiscf.

24. Queensland Government, 2021, *Information and cyber security policy (IS18)*, viewed 28 October 2023, www.forgov.qld.gov.au/information-technology/queensland-government-enterprise-architecture-qgea/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/information-security-policy-is18.

25. European Union, 2018, *EU GDPR*, viewed 28 October 2023, https://gdpr-info.eu/.

26. Queensland Office of the Information Commissioner, 2025, *Undertaking a Privacy Impact Assessment*, viewed 28 October 2023, www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-impact-assessments/undertaking-a-privacy-impact-assessment.

27. Queensland Government, 2021, *Information management policy framework*, viewed 28 October 2023, www.forgov.qld.gov.au/information-technology/queensland-government-enterprise-architecture-qgea/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/information-management-policy-framework.

28. Queensland Government, 2021, *ICT asset disaster recovery planning guideline*, viewed 28 October 2023, www.forgov.qld.gov.au/information-technology/queensland-government-enterprise-architecture-qgea/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/ict-asset-disaster-recovery-planning-guideline.

29. Queensland Government, 2009, *Right to Information Act 2009*, viewed 28 October 2023, www.legislation.qld.gov.au/view/pdf/current/act-2009-013.

30. Queensland Government, 2002, *Public Records Act 2002*, viewed 28 October 2023, www.legislation.qld.gov.au/view/pdf/2023-03-01/act-2002-011.

31. Queensland Government, 2021, *Metadata management principles*, viewed 28 October 2023, www.forgov.qld.gov.au/information-technology/queensland-government-enterprise-architecture-qgea/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/metadata-management-principles.

32. Queensland Government, 2021, *Metadata schema for Queensland Government assets guideline*, viewed 28 October 2023, www.forgov.qld.gov.au/information-technology/queensland-government-enterprise-architecture-qgea/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/metadata-schema-for-queensland-government-data-assets-guideline.

33. Queensland Government, 2010, *Public Interest Disclosure Act 2010*, viewed 28 October 2023, www.legislation.qld.gov.au/view/html/inforce/current/act-2010-038.

34. Queensland Government, 2009, *Financial Accountability Act 2009*, viewed 28 October 2023, www.legislation.qld.gov.au/view/html/inforce/current/act-2009-009.

35. Queensland Government, 2019, *Financial and Performance Management Standard 2019*, viewed 28 October 2023, www.legislation.qld.gov.au/view/html/inforce/current/sl-2019-0182.

36. Queensland Government, 2024, *Building Policy Framework*, viewed 28 October 2023, www.forgov.qld.gov.au/property-land-and-infrastructure/manage-government-buildings-and-assets/building-frameworks/building-policy-framework.

37. Queensland Treasury, 2023, *Queensland Treasury Strategic Plan 2023-2027*, viewed 28 October 2023, https://s3.treasury.qld.gov.au/files/QT-Strategic-Plan-2023-2027.pdf.

38. Queensland Treasury, 2020, *A Guide to Risk Management*, viewed 28 October 2023, www.treasury.qld.gov.au/resource/guide-risk-management.

39. Queensland Government, 2001, *Crime and Corruption Act 2001*, viewed 28 October 2023, www.legislation.qld.gov.au/view/html/inforce/current/act-2001-069.

40. Queensland Government, 2009, *Integrity Act 2009*, viewed 28 October 2023, www.legislation.qld.gov.au/view/pdf/current/act-2009-052.

41. Queensland Government, 2021, *Digital Governance Investment Framework*, viewed 28 October 2023, www.forgov.qld.gov.au/information-technology/queensland-government-enterprise-architecture-qgea/digital-investment-governance-framework.

42. Australian Cyber Security Centre, 2023, *AI Data Security*, viewed 28 October 2023, www.cyber.gov.au/resources-business-and-government/governance-and-user-education/artificial-intelligence/ai-data-security.

43. National Institute of Standards and Technology, 2002, *NIST FIPS 140-2 Security Requirements for Cryptographic Modules*, viewed 28 October 2023, https://csrc.nist.gov/pubs/fips/140-2/upd2/final.

44. National Institute of Standards and Technology, 2020, *NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations*, viewed 28 October 2023, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

45. National Institute of Standards and Technology, 2023, *NIST AI Risk Management Framework*, viewed 28 October 2023, www.nist.gov/itl/ai-risk-management-framework.

Queensland Government

FRONTIER SI