ACT Government Artificial Intelligence Policy

Version 0.1

July 2024

We acknowledge the Ngunnawal people as traditional custodians of the ACT and recognise any other people or families with connection to the lands of the ACT and region. We acknowledge and respect their continuing culture and the contribution they make to the life of this city and this region.

Introduction

Background

Artificial Intelligence (AI) is the capability of computer systems to perform reasoning and solve complex problems. The CSIRO Artificial Intelligence Roadmap (2019) highlighted AI applications across Australia, particularly within government sectors. The recommendations emphasise the importance of specialising in, investing in, and using AI technologies.

For government, AI presents opportunities to:

- enhance policy and service design and delivery
- streamline regulatory and compliance functions
- improve operational management of organisations' digital and data assets
- address complex, multidisciplinary challenges.

AI's fast adoption may also introduce risks, for example bias, privacy, governance and accountability. This could undermine the community's trust and willingness to engage with ACT government services. As the technology rapidly evolves and the ACT Government advances to more mature and complex uses of AI, we must develop appropriate governance processes to support initiatives and meet the needs and expectations of our community.

Purpose

The ACT AI Policy (the Policy) establishes the ACT AI Assurance Framework (the Framework) to implement the National AI Ethics Principles and National AI Assurance Framework (NAIAF). Adopting the NAIAF means we meet key national standards and commit to maintaining community trust by developing AI solutions that are well-designed, safe, and appropriately governed.

Aligning with national standards also improves transparency and supports a consistent, efficient approach to AI development and implementation across the Australian public sector.

This Policy and the ACT AI Assurance Framework allows the ACT Government to identify and manage the risks associated with AI effectively. This Policy sets out how the ACT Government can:

- manage the ethical risks that arise from AI technology (discussed in the *Self-Assessment Template*)
- align the ACT's AI governance and usage to national commitments and to other Australian jurisdictions
- communicate its stance on AI with the community
- provide transparency on the use of AI within the ACT public sector
- leverage AI as a strategic asset to enhance efficiency and deliver solutions for the ACT community.

Scope

The Policy and Framework apply to **all** AI projects that:

- Use AI in commercially available products in **new and novel ways**. For example, creating a tailored solution specifically for the ACT Government (excludes configuration[1]). Standard usage of AI functionalities in commercially available solutions are exempt from this policy.[2]
- Use AI solutions **specifically developed** or trained for the ACT public service, internally or by external vendors.
- Use **generative AI capabilities**, even if these capabilities are part of standard commercially available products and are not modified.

In certain domains, the use of AI functionality in commercially available solutions may already be regulated by existing laws and regulations. For example, in the medical or clinical sector, AI usage may be subject to approval by the Therapeutic Goods Administration (TGA). These solutions do not fall under the scope of this policy.

ACTPS staff's use of AI tools, such as generative AI technologies, is also covered by complementary policies and guidance including:

- Artificial Intelligence: When to use it and when to avoid it at work
- the ACTPS Code of Conduct and all relevant Human Resources policies
- software usage regulations (for example, those governing Microsoft Outlook or the use of Smart Devices)
- all relevant legislation (notably the *Information Privacy Act 2014*).

What is AI?

AI is the capability of a computer system to use data and algorithms to perform tasks similar to the reasoning and processing tasks performed by human experts. These tasks currently include, but are not limited to:

- reasoning and planning
- natural language processing
- computer vision
- audio processing
- interaction
- identifying meaningful patterns
- decision-making
- prediction
- generating text, images, audio material, and videos.

AI can be designed and used to operate with varying levels of automation. These technologies include, but are not limited to:

[1] Excluding configuration means that the policy does not apply to basic setup or customisation of AI products that are already commercially available.

[2] Standard use AI functionalities as they are intended and provided by the vendor, without any modifications or special customisations are exempt from the policy because they are routine and do not involve new or novel applications. For example, using a built-in AI feature in a software application for its intended purpose, like automated email sorting in an email client, would be considered standard use.

- **Machine learning**, enabling computer systems to learn from data.
- **Computer vision**, allowing computer systems to interpret visual information.
- **Natural language processing**, assisting in understanding and generating human language.
- **Generative AI**, producing audio, visual, text or code content with minimal intervention.

Key terms

- **AI technology** – An encompassing term that refers to the algorithms, tools, and techniques used to create or train AI models and the AI systems and AI models themselves.
- **AI model** – A program that employs AI algorithms and techniques to solve complex tasks.
- **AI system** – A group of interacting elements of which at least one is an AI model. In the case of Generative AI, the system includes but is not limited to the Large Language Model and the corpus of knowledge used by the model to generate an output.
- **AI solution** – The development of an AI system as a solution to a particular problem or problems.

Roles and responsibilities

Responsible Officers

The Policy defines the roles of **Responsible Officers** for AI solutions. Eligible AI projects must identify **four** Responsible Officers, each bringing a unique role and perspective for comprehensive oversight and management.

Each role is **independent** and **should be assigned a different person**.[3] Responsible Officers should be senior, skilled, and qualified.

Responsible Officer's roles and responsibilities are similar to those in the Cyber Security Policy but have been tailored to requirements of this policy. Shared responsibilities are not duplicated – meeting the requirements of one role automatically satisfies the other.

Table 1 lists each Responsible Officer's responsibilities and any overlaps in responsibilities.

Table 1. The responsibilities of each Responsible Officer.

Responsible Officer	Responsibilities
AI System Owner ***(overlaps with 'Business System Owners')***	Person at executive or senior level within an administrative unit with the authority to: • oversee AI system insights and decisions • define the strategy • align goals and deliverables • ensure compliance with framework requirements • take responsibility for the project's outcomes.

[3] This requirement may not be suitable for small-scale projects. In this case, any known risks arising from an individual occupying more than one 'Responsible Officer' role should be documented in the Self-Assessment, noting all mitigations in place.

AI System Administrator *(overlaps with 'System Administrator')*	An ACTPS officer with access privileges, knowledge, and skills necessary to manage and monitor the AI system's technical performance and deploy updates and changes.
Data Custodian/Steward	An ACTPS officer responsible for the data used in an AI system and meeting data governance and management requirements.
Project Managers	An ACTPS officer who manages the AI system project scope, goals, and deliverables.

To comply with the Policy, directorates must provide **bi-annual summaries of their AI projects** to the ACT AI Advisory Group for inclusion in an AI register. An abridged version of the AI register may be made public.[4]

At a minimum, these summaries must include:

- A brief description of the project and how AI is used.
- Key ethical considerations taken in designing the project.
- A contact point (preferably a team or office's group email address or phone number).

The Secretariat of the AI Advisory Group will manage details of this reporting arrangement. This includes the requesting and collection of information, and the administration of the public facing register.

Directorates should also **nominate and document** their project's Responsible Officers, in line with record keeping requirements.

To better integrate these roles, directorates can include their responsibilities or titles in relevant position descriptions. Additionally, they can develop directorate-specific policies outlining any additional responsibilities related to AI solutions or projects.

Other relevant roles

There are other relevant roles essential for aligning, securing, and implementing AI technologies across the ACT Government. They focus on overarching strategies and coordination, providing leadership, governance, and technical oversight.

These roles work **collaboratively with the Responsible Officers** outlined in the Policy to integrate AI solutions into our operations while maintaining compliance and security standards. Table 2 describes each role.

Table 2. The responsibilities of the other relevant roles.

Role	Responsibilities

[4] A project is exempt from this reporting requirement if disclosing the nature of an AI-system is deemed inappropriate from a public safety perspective. For example, if a cyber security solution uses an AI component, knowledge of that fact could help a malicious threat actor.

ACT Chief Digital Officer (CDO)	• Develop and drive strategic digital solutions and strategies to enhance service delivery. • Set the vision and strategy for AI adoption and governance by ensuring alignment with digital strategy.
Chief Information Security Officer (CISO)	• Provide cyber security advice to project proposals as part of the AI Advisory Group, as required.
Chief Information Officers (CIOs)	• Promote the responsible adoption of AI technologies within their directorate. • Oversee the use of AI tools within their directorates. This includes relevant cyber security mitigations, and any ethical considerations and required actions. • Maintain a register of all AI tools used in their directorate (as part of their reporting commitment to the AI Advisory Group).
	•
Digital, Data and Technology Solutions (DDTS)	• Develop and implement ACT digital strategy, cyber security, and ICT policies. • Create and implement technology solutions, drive the use of data, oversee ICT investments, and provide ICT infrastructure and services.
Directors-General and agency heads	• Set the strategic direction for their directorate in line with government objectives. • Support and provide resources for AI initiatives as required. • Take full responsibility for the safe and responsible deployment of AI in their directorates.
ICT Project Managers (DDTS)	• Support ICT projects and operations, including AI technologies, and liaising between DDTS and directorate-based staff. Note: not all projects involve DDTS or ICT Managers.

ACT AI Advisory Group

This policy establishes the **ACT AI Advisory Group (AIAG)** to support the ethical development and roll out of AI across the ACT Government.

The AIAG will assist in the ethical use of AI solutions to maintain the trust of the community. It will operate concurrently with existing ICT review and governance processes.

The AIAG has the following **roles and responsibilities**:

- Assess that AI solutions ‘in scope’ as defined by the AI policy and framework meet ethical requirements in line with the national AI assurance commitments, and ACT-specific human rights, wellbeing, environmental and workforce considerations,
- advise project sponsors and managers on the ethical feasibility of certain AI projects, offering guidance to mitigate ethical risks assessed as medium, and to reconsider or pause high-risk projects,
- suggest revisions to AI project proposals to meet the above standards,
- provide input into the strategic direction of AI capability across the service, and on the usage and rollout of AI capability and tools, for example Copilot365,
- support the design of AI risk assessment tools, and
- report on the use of AI across government.

Table 3 describes the composition of the AIAG.

To support whole of government consistency and capability, directorates can incorporate the AIAG as a function into their AI-related directorate governance processes. Directorates are also encouraged set up their own governance processes for AI projects prior to their submission to the AIAG.

Table 3. The members and respective responsibilities of the AIAG.

Member	Responsibilities
Chair and Co-chair	• Chair: Executive Group Manager, CDT, DDTS. • Co-chair: Executive Branch Manager, Digital Strategy, Services & Transformation, Education. • Appointed by DRG for 12 months. Secretariat leads reviews and DRG will confirm appointments.
Directorate Representatives	• Ex-officio appointments for 24 months. Meeting proxies allowed, when necessary, with Secretariat approval. • Standing members: Executive Branch Managers from Access Canberra and Data, AI and Digital Records (DAIDR)/DDTS. • Additionally, one representative at Executive Branch Manager level from each Directorate, nominated by their directorate’s DRG representative. Members may oversee their directorate’s rollout of AI. • Members represent their directorate and conduct all required internal consultation, and briefing processes to the relevant DDG/DG through established directorate-specific channels. They provide insights and recommendations on behalf of their directorates, including conducting directorate-level consultation on proposals, as applicable.
AI Subject Matter Experts	• Up to four subject matter experts. They are nominated by directorates and appointed by the Chair and Co-chair, on advice from the Executive Branch Manager, DAIDR.

Additional specialist members	• Up to four ex-officio members. • To ensure a comprehensive focus on human rights, wellbeing, legislation, legal, and policy aspects, the following additional members will be included as ex-officio members who may send proxies when necessary: ▪ A representative from the Wellbeing team, CMTEDD. ▪ A representative from the ACT Human Rights Commission, JACS. ▪ A legal advisor from the Legal Services unit, JACS. ▪ A representative from the Office for Industrial Relations and Workforce Strategy (OIRWS).
Secretariat	• Lead roll-out of AI capability across the ACT Public Service. • Drive the strategic agenda of the AIGG, in partnership with the Chair and Co-chair, and under mandate from DRG. • Manage end to end secretariat support for the Group. • Performed by the DDTS Data, AI, and Digital Records Branch.
Guests and Presenters	• Presenters, guests, and observers may be invited to attend certain meetings, sponsored by a member, and approved by the Chair. They will not become standing AIAG members.

Relevant legislations, policies, and other documents

Table 4. The other relevant documents to consider.

Legislation and policy	Description
National AI Assurance Framework	The National AI Assurance Framework establishes a joint approach, based on the national ethics principles, to safe and responsible AI. The Framework was agreed by Australian Data and Digital Ministers on 21 June 2024.
Human Rights Act	The ACT Human Rights Act protects and promotes human rights. AI system owners, especially those in criminal justice, education, and detention contexts, should consider whether the AI system may infringe on an individual's rights.
Information Privacy Act	The Information Privacy Act sets out the Territory Privacy Principles (TPPs), which govern how the ACT Government collects and uses data. This is important to AI systems trained on data.
Public Sector Management Act .	The Public Sector Management Act of the ACT regulates the administration of the public sector in the Territory including establishing the standards for public service jobs, public sector values and principles. The PSM Act also provide the mechanism for handling changing in structures and positions.

ACT Wellbeing Framework	The ACT Wellbeing Framework informs our implementation of the National AI Ethics Principles by establishing an understanding of what impacts quality of life. Alignment ensures advancements in AI and community wellbeing are ethical, reliable, and centred on improving quality of life for all Canberrans.
Data Governance and Management Framework and other standards	The Data Governance and Management Framework (DGMF) supports the ACT Government develop its data maturity to deliver better outcomes for the community.
Cyber Security Policy	The ACT Cyber Security Policy is essential to protecting data used by all ACT Government ICT systems, including AI systems. It aligns with the ACT Government Protective Security Policy Framework, ensuring that sensitive information is protected against unauthorised access and disruptions. This policy establishes security standards, enabling the secure and ethical deployment of AI technologies, ensuring compliance with government data protection obligations, and maintaining public trust.
Data Sharing Policy	Relevant to AI systems that use data from other agencies. The Data Sharing Policy defines the requirements for data sharing agreements within the ACT Government and with external entities. It ensures that data used in AI systems is deployed in a manner that is safe, legal, and trusted by the community.
ACT Digital Strategy	The ACT Digital Strategy sets out how the ACT Government will design AI services with the community in mind, leveraging technology to improve our quality of life and making Canberra a more liveable, sustainable, and connected city.

AI Ethics Principles

The Policy adheres to the National AI Ethics Principles, guiding the ACT Government's use of AI. This alignment ensures the ACT meets national standards and community expectations regarding the ethical use of AI by the government.

AI Assurance Framework

This Policy establishes the ACT AI Assurance Framework as the document that **governs all development and customisation of AI for the ACT Government**.

This Framework draws on the National and NSW AI Assurance Frameworks. The Framework sets out the process for ACT Government directorates to self-assess their AI projects throughout their lifecycle. This ensures appropriate consideration of ethical principles, security, privacy, and accountability.

Scope

The Policy and Framework apply to **all** AI projects that:

- Use AI in **commercially available products in new and novel ways**. For example, the solution is tailored for a new use, specifically for the ACT public service (excluding configuration). Standard usage of AI functionality in commercially available solutions is exempt from this policy.
- Use AI solutions **specifically developed or trained for the ACT public service**, whether developed by internal staff or external vendors.
- Use generative AI **capabilities**, even if these capabilities are part of standard commercially available products and are not modified.

Only projects that receive a '**medium'** or '**high'** risk rating must submit their completed self-assessment to the AIGG for review. Approval to proceed through the regular DDTS project lifecycle governance will be granted, or recommendations on project risk management will be issued by the AIGG, based on this review.

The self-assessment process established under the Framework must be applied to all eligible AI projects **during their planning stages**. This includes consideration of planning, delivery, and review phases. This is recommended for ongoing compliance, especially when significant changes to the solutions occur, for example, major upgrades.

Key aspects of the Framework include:

- Comprehensive risk analysis and documentation of AI-specific risks.
- Supports to identify risks and begin developing risk mitigation strategies.
- Establishment of clear governance and accountability measures for AI projects.

Intended users of the Framework include:

- Project teams deploying AI
- Operational teams managing AI
- Officers responsible for AI design and use
- Internal assessors for self-assessments
- Directorate-level (ICT) governance teams
- The AI Advisory Group

ACTPS Requirements under the AI Policy

ACTPS staff designing, administering, or operating an AI System in the ACT Government ICT environment must use the Assurance Framework established by this Policy. Under the Assurance Framework, ACTPS staff must ensure that they:

- Develop and use AI initiatives in alignment with directorate strategic plans, and broader ACT government priorities.
- Demonstrate community or government advantages, such as improved service delivery or enhanced decision-making capabilities.
- Comply with all relevant privacy, security, and data protection laws.
- Implement strategies to minimise potential biases and risks in AI algorithms.
- Ensure that decisions made by the AI system are subject to human review and intervention.

AI Assurance Framework

Introduction

This Policy establishes the ACT AI Framework as the document that **governs all development and customisation of AI for the ACT Government**. This Framework draws on the National and NSW AI Assurance Frameworks.

What is the AI Assurance Framework?

The Framework aims to support the ACT Government to innovate with AI solutions, while ensuring ethical, secure, and accountable measures for the design and usage of AI solutions.

The Framework will help ACTPS staff design, build, and use AI technology appropriately. It contains questions for staff to answer at every stage of their project. If you cannot answer a question, the Framework guides you to several resources and points of further information to help develop your response.

Who should use it?

The Framework is intended to be used by:

- project teams who are using AI systems in their solutions
- operational teams who are managing AI systems
- responsible officers who are accountable for the design and use of AI systems
- internal assessors conducting agency self-assessments
- the AI Advisory Group, in their assessment of proposed projects.

When should I use it?

All AI systems and projects must be assessed against the Framework, and consider all stages of an AI project, from initial planning to delivery. Regular reviews should be conducted to review services that use AI systems, in addition to any existing service review processes.

Is applying this framework everything I need to do?

The Framework is not a complete list of all requirements for AI projects. Project teams should comply with their directorate-specific AI processes, policy requirements, and any other directorate or whole of government ICT governance and assurance mechanisms.

When you do not need to apply this framework

Except for Generative AI solutions, you do **not** need to assess your product or service if:

- You are using an AI system that **is a widely available commercial application**. For example, virtual assistants, fraud detection systems, image and speech recognition.
- You are **not customising the AI system in any way**, or using it beyond its intended purpose. For example, using ACT Government-controlled data to train and/or maintain the AI mode is considered customisation and requires assessment.

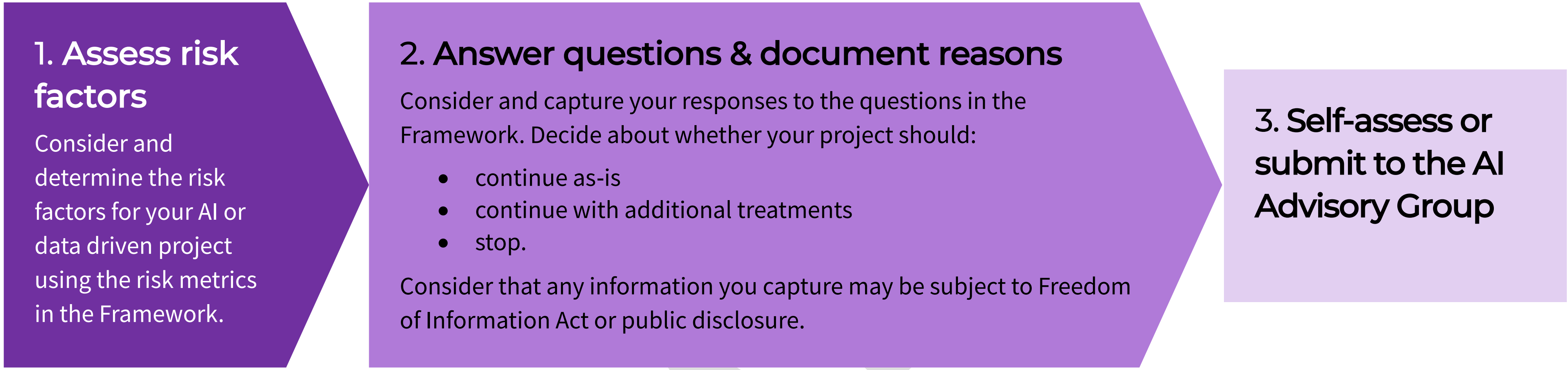
How to conduct an AI assurance assessment

This assessment is to be completed by (or the result confirmed with) the Responsible Officers. See **Table 1** for the responsibilities of each Responsible Officer.

At the end of the self-assessment, the template will assign a risk rating (highest risk and total number of risks ranked medium or higher) to the different principles in your AI project. This rating will determine if your project should proceed as is, or if you should make a submission to the AI Advisory Group for consideration. See **Figure 1** for a summary of the steps needed to conduct an AI assurance assessment.

Eligible AI projects must identify four Responsible Officers, each bringing a unique role and perspective for comprehensive oversight and management. Each role is independent and should not be held by the same person.[5] Responsible Officers should be senior, skilled, and qualified.

[5] This requirement may not be suitable for small-scale projects. In this case, any known risks arising from an individual occupying more than one 'Responsible Officer' role should be documented in the Self-Assessment, noting all mitigations in place.



1. Assess risk factors

Consider and determine the risk factors for your AI or data driven project using the risk metrics in the Framework.

2. Answer questions & document reasons

Consider and capture your responses to the questions in the Framework. Decide about whether your project should:

- continue as-is
- continue with additional treatments
- stop.

Consider that any information you capture may be subject to Freedom of Information Act or public disclosure.

3. Self-assess or submit to the AI Advisory Group

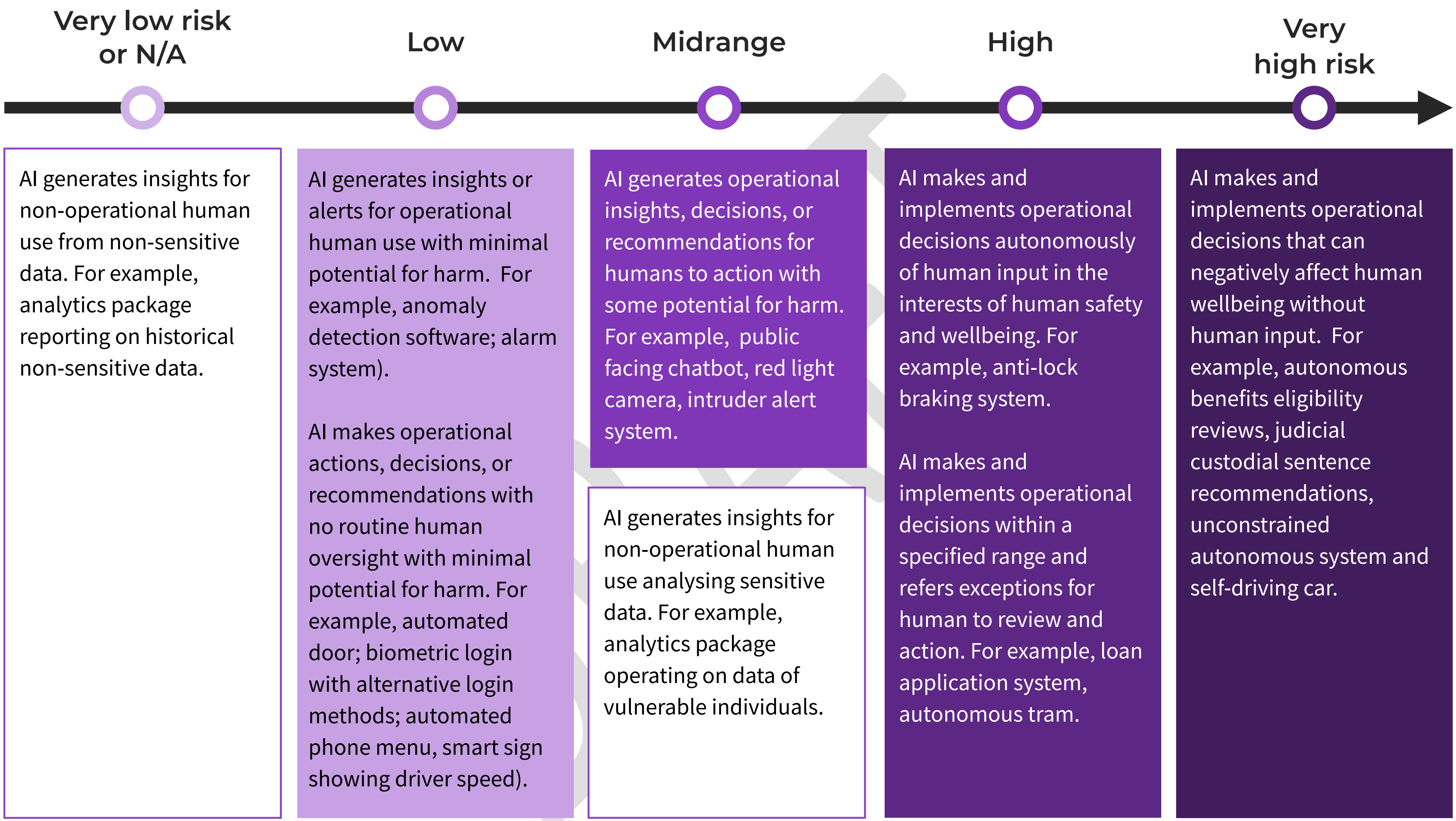
Figure 1. The steps to conduct an AI assurance assessment.

Evaluating AI benefits and risks

The ACT Government has a strong commitment to the responsible use of technology. This Framework is structured to support risk and benefit assessments across each of the 8 AI Ethics Principles. Every section starts with prompts to help you consider the types of risk that your project may carry. Every section of the self-assessment includes prompts to help you consider the types of risk that your project may carry. Following these prompts will allow you to shape your responses clearly and ensure your project meets ethical requirements. .

AI Risk Spectrum

Figure 2 describes the AI risk spectrum. The key factor that determines risk is how the AI system is used, including whether it has an operational impact, or is not transparent, explainable, and traceable.



Very low risk or N/A

AI generates insights for non-operational human use from non-sensitive data. For example, analytics package reporting on historical non-sensitive data.

Low

AI generates insights or alerts for operational human use with minimal potential for harm. For example, anomaly detection software; alarm system).

AI makes operational actions, decisions, or recommendations with no routine human oversight with minimal potential for harm. For example, automated door; biometric login with alternative login methods; automated phone menu, smart sign showing driver speed).

Midrange

AI generates operational insights, decisions, or recommendations for humans to action with some potential for harm. For example, public facing chatbot, red light camera, intruder alert system.

AI generates insights for non-operational human use analysing sensitive data. For example, analytics package operating on data of vulnerable individuals.

High

AI makes and implements operational decisions autonomously of human input in the interests of human safety and wellbeing. For example, anti-lock braking system.

AI makes and implements operational decisions within a specified range and refers exceptions for human to review and action. For example, loan application system, autonomous tram.

Very high risk

AI makes and implements operational decisions that can negatively affect human wellbeing without human input. For example, autonomous benefits eligibility reviews, judicial custodial sentence recommendations, unconstrained autonomous system and self-driving car.

Figure 2. The AI risk spectrum.