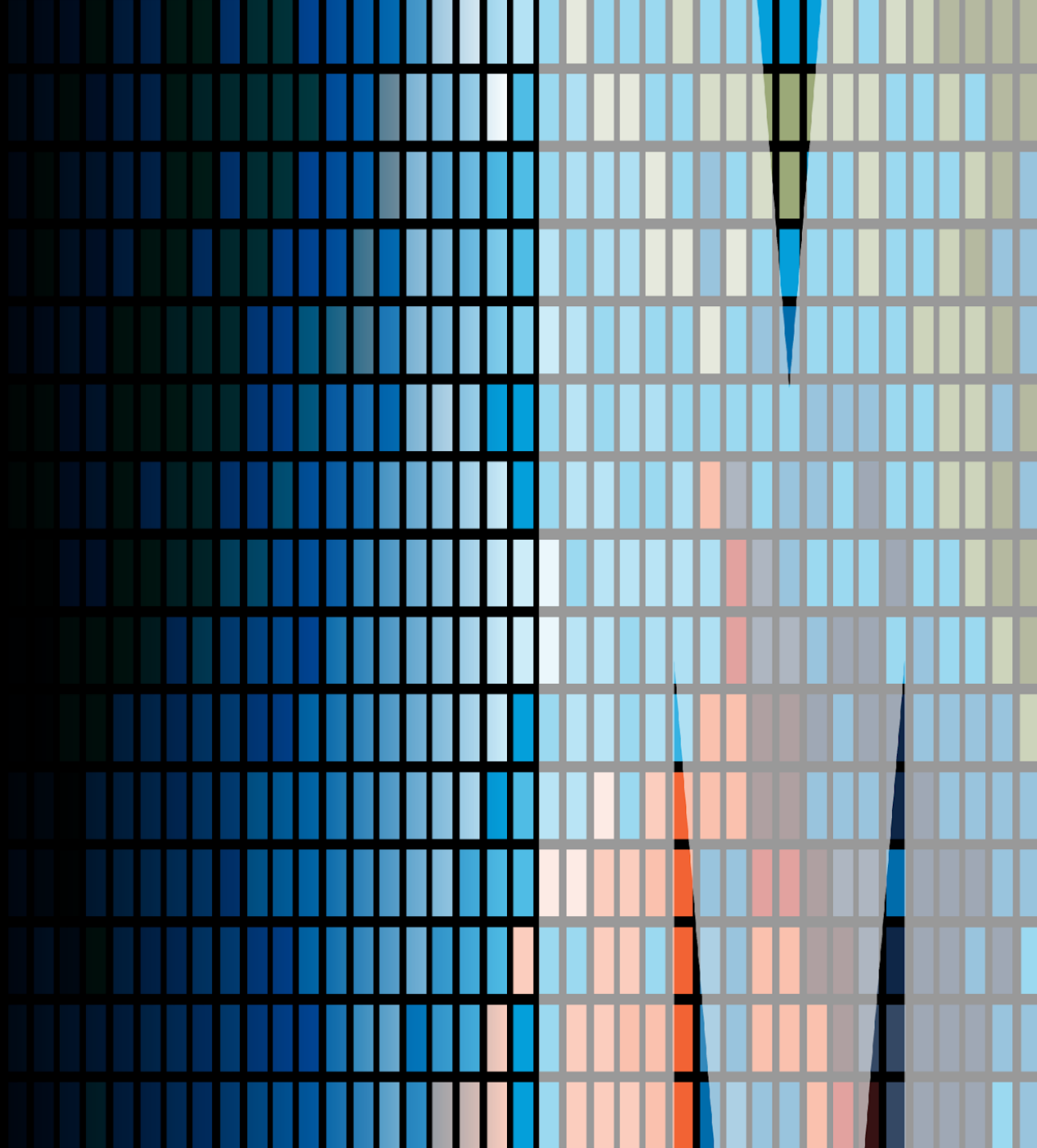
MONASH University

AI-Ready Research Data in Australia

Research Data Strategy
Office of PVC-RI

October 2025

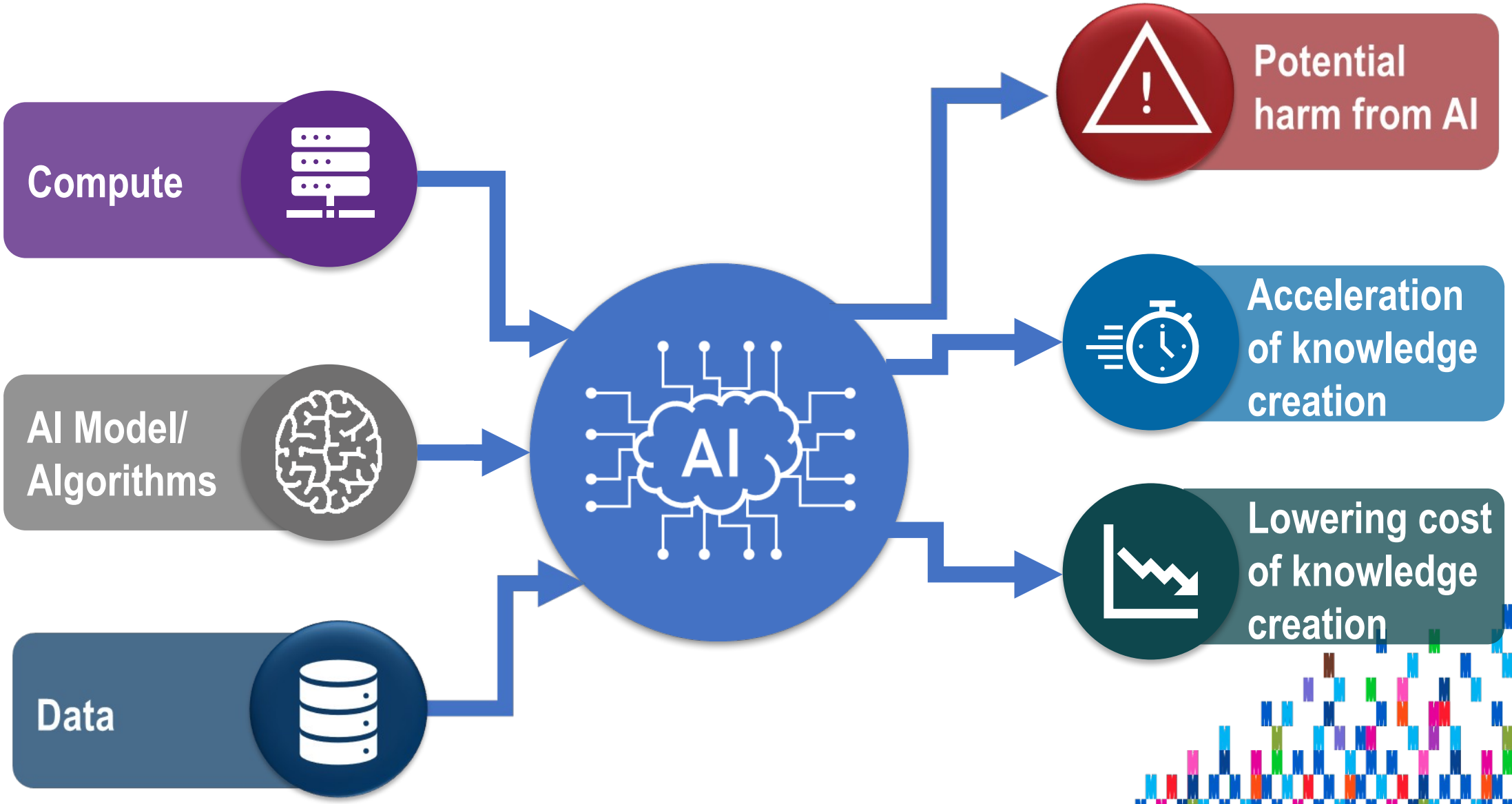
Dianne Brown
Komathy Padmanbhan



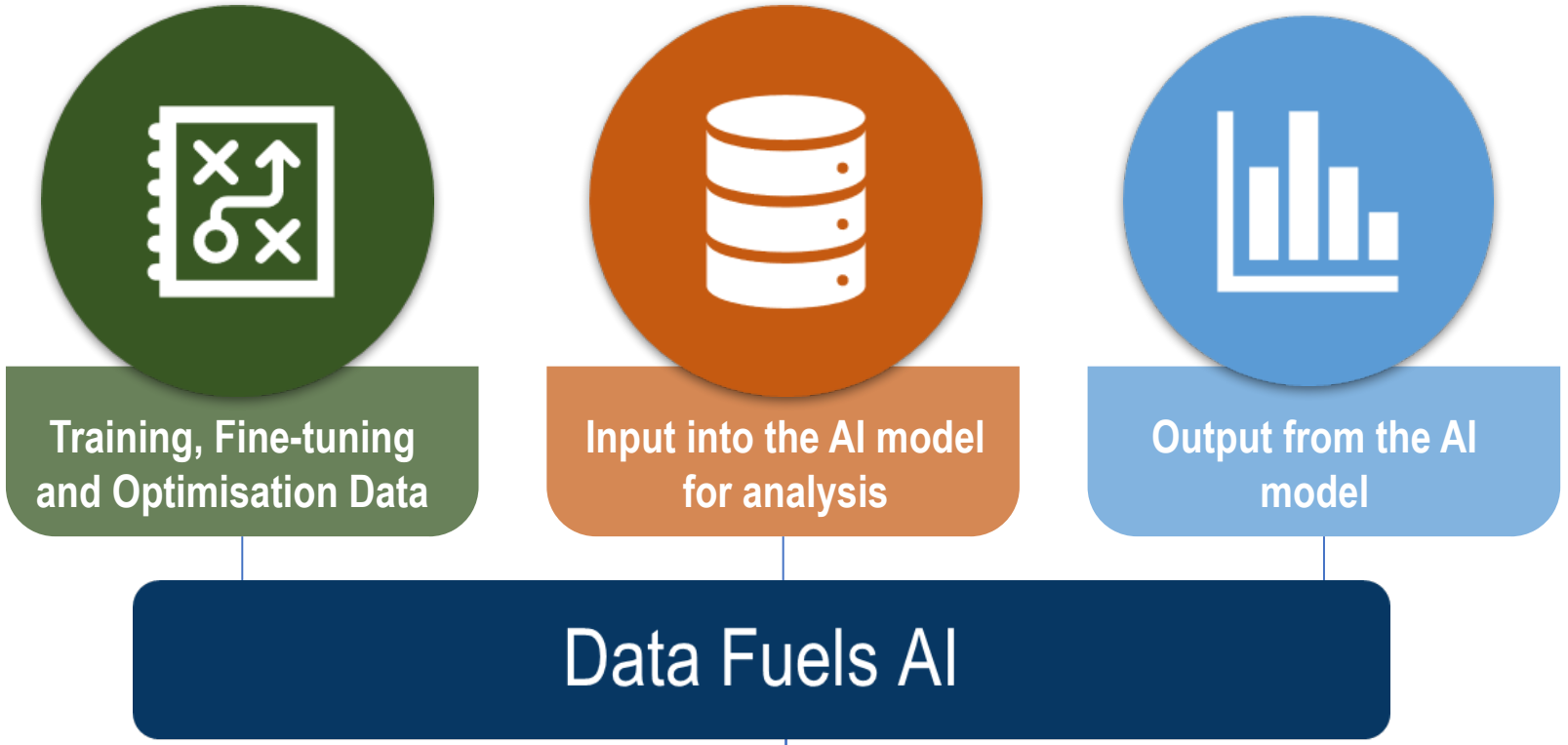
MONASH University

MONASH UNIVERSITY recognises that its Australian campuses are located on the unceded lands of the people of the Kulin nations, and pays its respects to their Elders, past and present.

AI is reshaping the world and research

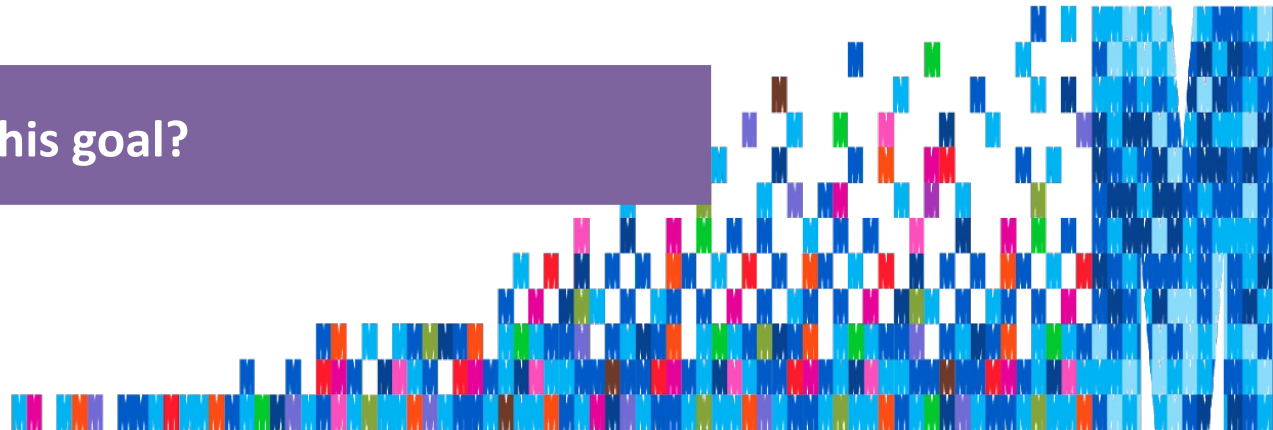


Data's Role


Training, Fine-tuning and Optimisation Data
Input into the AI model for analysis
Output from the AI model
Data Fuels AI
AI

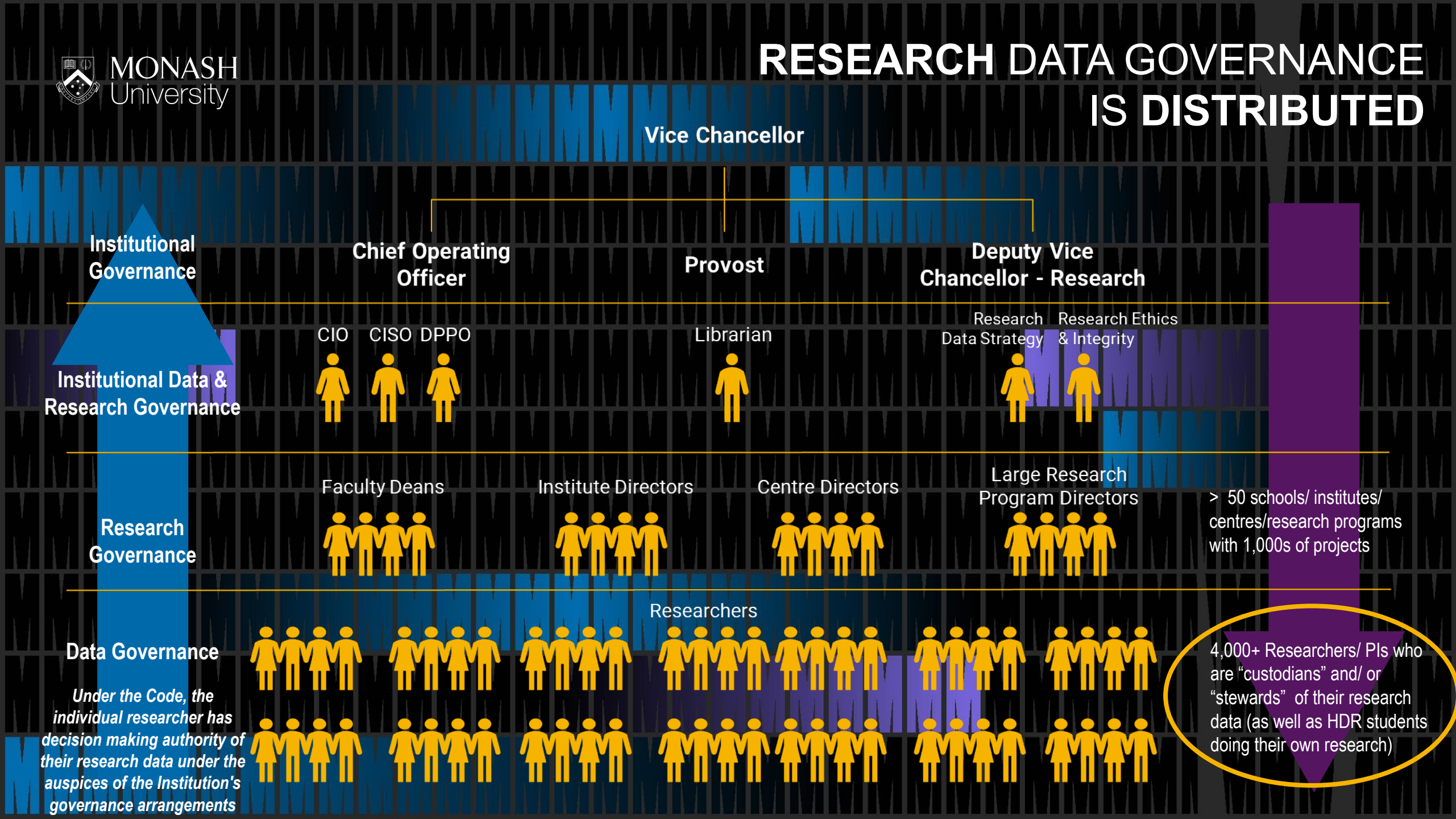
Questions for today

- What do we mean by “AI-ready research data”?
- What type of application of AI are we talking about?
- Should focus be on opportunity or risk?
- How do we arrive at this goal?



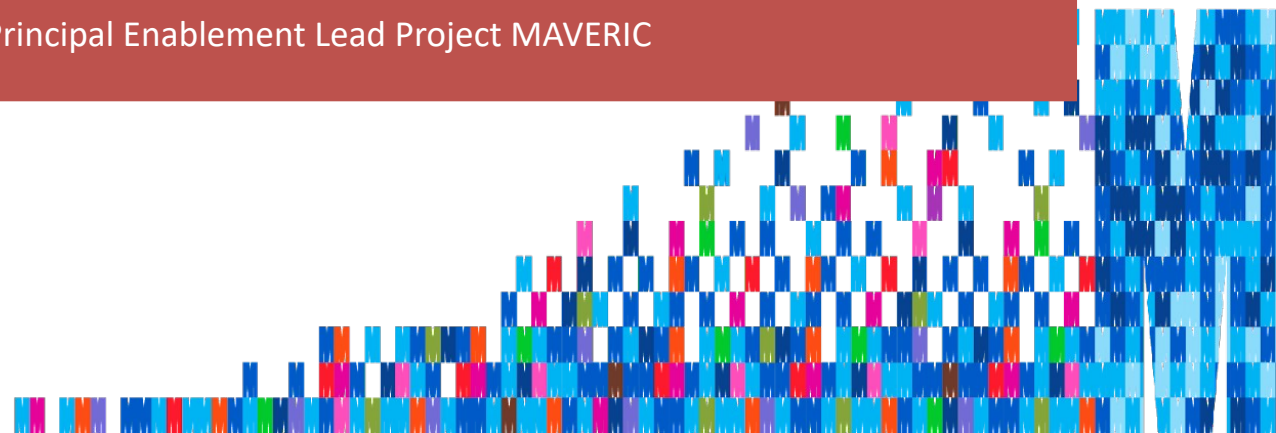
MONASH University

RESEARCH DATA GOVERNANCE IS **DISTRIBUTED**

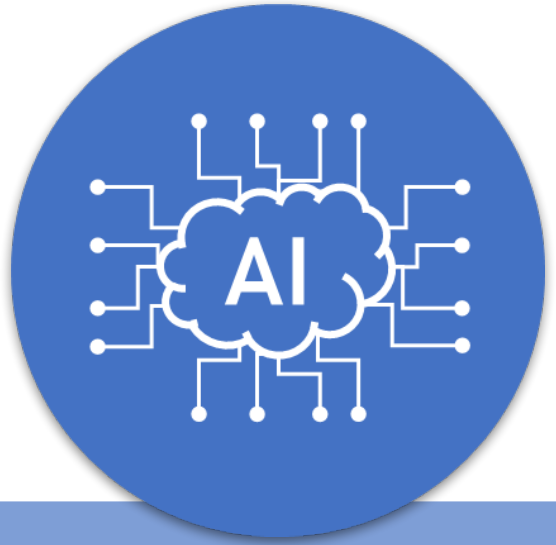


Current state at 3 institutions

Jacky Cho	Manager (Research data and software), Research Technology Services
Prof Paul Bonnington	Pro-Vice Chancellor (Research and Infrastructure)
Gin Tan	Principal Enablement Lead Project MAVERIC



Panel Discussion



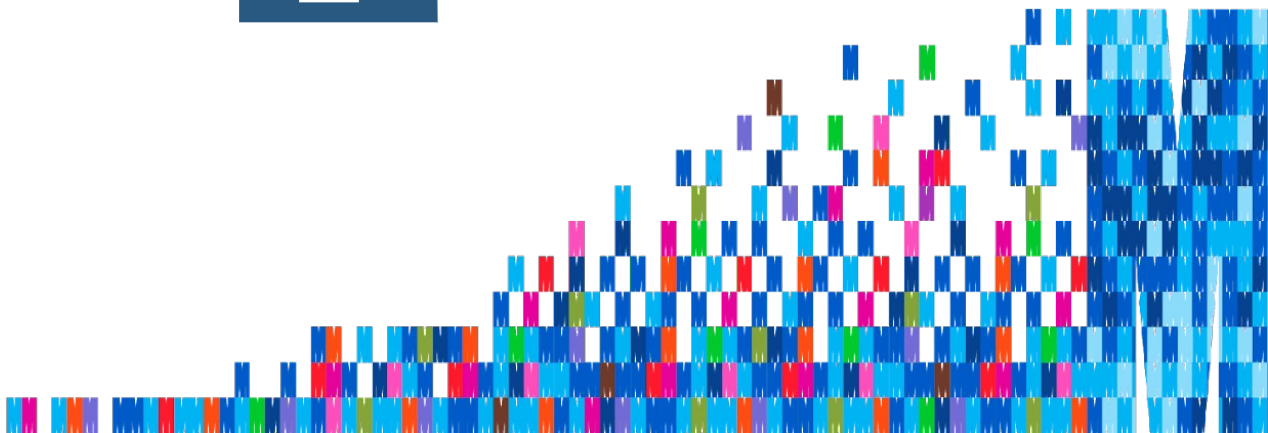
Can we collaborate and progress the development of an ***AI-ready research data framework*** *for institutions, including:*

- *governance,*
- *support systems and*
- *workforce capabilities*

Is it needed? Achievable?

Can we agree on definition?

Where should we focus?



MONASH University

Next Steps?

Australian AI Ethical Principles

Human, societal and environmental wellbeing: AI systems should benefit individuals, society and the environment

Human-centred values: AI systems should respect human rights, diversity, and the autonomy of individuals.

Fairness: AI systems should be inclusive and accessible, and should not involve or result in unfair discrimination against individuals, communities or groups.

Privacy protection and security: AI systems should respect and uphold privacy rights and data protection, and ensure the security of data

Reliability and safety: AI systems should reliably operate in accordance with their intended purpose.

Transparency and explainability: There should be transparency and responsible disclosure so people can understand when they are being significantly impacted by AI, & can find out when an AI system is engaging with them

Contestability: When an AI system significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or outcomes of the AI system.

Accountability: People responsible for the different phases of the AI system lifecycle should be identifiable and accountable for the outcomes of the AI systems, and human oversight of AI systems should be enabled.

Australian Government. Australia's Artificial Intelligence Ethics Principle: Department of Industry Science and Resources,; 2019 [updated 11 October 2024. Available from: https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-principles.

12 NIST GenAI Risks

CBRN Information or Capabilities

Eased access to or synthesis of materially nefarious information or design capabilities related to chemical, biological, radiological, or nuclear (CBRN) weapons or other dangerous materials or agents.

Confabulation

The production of confidently stated but erroneous or false content (known colloquially as "hallucinations" or "fabrications") by which users may be misled or deceived.

Dangerous, Violent or Hateful Content

Eased production of and access to violent, inciting, radicalizing, or threatening content as well as recommendations to carry out self-harm or conduct illegal activities. Includes difficulty controlling public exposure to hateful and disparaging or stereotyping content.

Data Privacy

Impacts due to leakage and unauthorized use, disclosure, or de-anonymization of biometric, health, location, or other personally identifiable information or sensitive data.

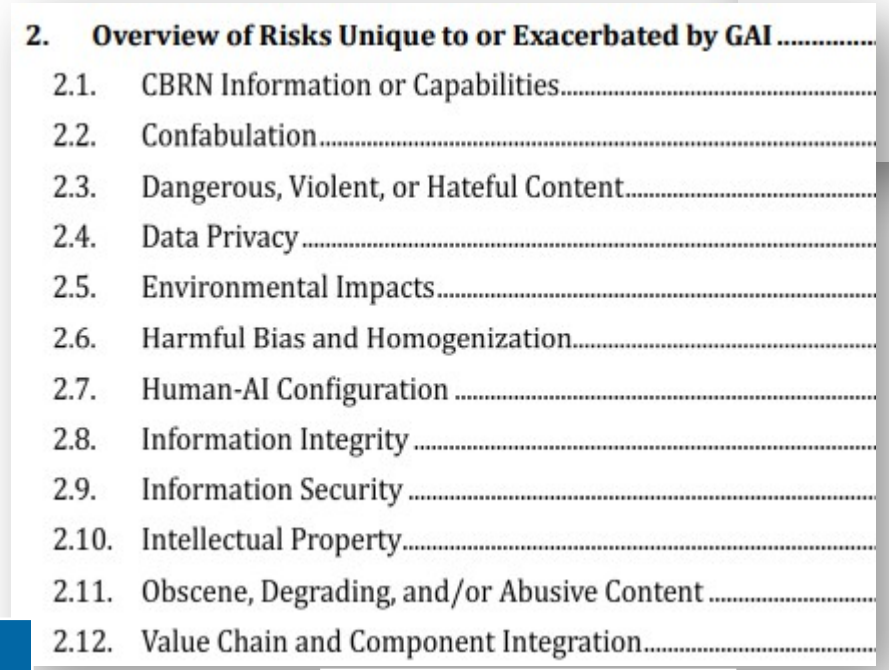
Environmental Impacts

Impacts due to high compute resource utilisation in training or operating AI models, and related outcomes that may adversely impact ecosystems

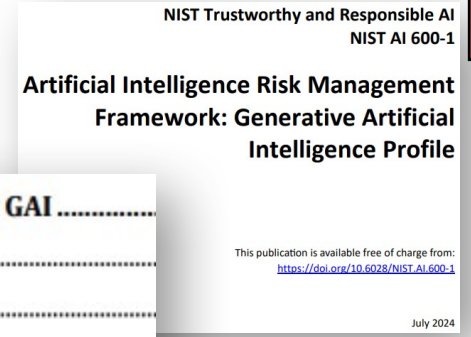
Harmful Bias or Homogenization

Amplification and exacerbation of historical, societal, and systemic biases

NIST AI RMF: Generative AI Profile



2. Overview of Risks Unique to or Exacerbated by GAI .....
- 2.1. CBRN Information or Capabilities.....
- 2.2. Confabulation.....
- 2.3. Dangerous, Violent, or Hateful Content.....
- 2.4. Data Privacy.....
- 2.5. Environmental Impacts.....
- 2.6. Harmful Bias and Homogenization.....
- 2.7. Human-AI Configuration .....
- 2.8. Information Integrity .....
- 2.9. Information Security .....
- 2.10. Intellectual Property.....
- 2.11. Obscene, Degrading, and/or Abusive Content .....
- 2.12. Value Chain and Component Integration.....



NIST Trustworthy and Responsible AI
NIST AI 600-1

Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile

This publication is available free of charge from: https://doi.org/10.6028/NIST.AI.600-1

July 2024

Human-AI Configuration

Interactions between a human and an AI system which can result in the human anthropomorphizing GAI systems or experiencing algorithmic aversion, automation bias, over-reliance, or emotional entanglement

Information Integrity

Lowered barrier to entry to generate and support the exchange and consumption of content which may not distinguish fact from opinion or fiction or acknowledge uncertainties. Loss of data providence

Information Security

Lowered barriers for offensive cyber capabilities; increased attack surface for targeted cyberattacks

Intellectual Property

Eased production or replication of alleged copyrighted, trademarked, or licensed content without authorization (possibly in situations which do not fall under fair use); eased exposure of trade secrets; or plagiarism or illegal replication.

Obscene, Degrading, and/or Abusive Content

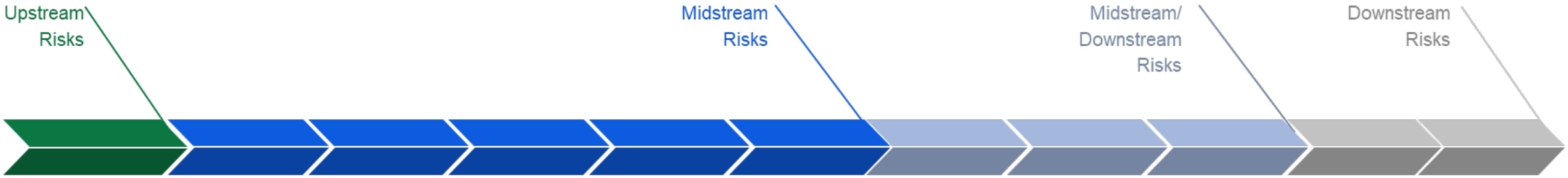
Eased production of and access to obscene, degrading, and/or abusive imagery which can cause harm, including synthetic child sexual abuse material (CSAM), and nonconsensual intimate images (NCII) of adults

Value Chain/ Component Integration

Non-transparent or untraceable integration of upstream components, including data that has been improperly obtained or not processed or other issues that diminish transparency or accountability for downstream users.

Source: United States Government. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. In: National Institute of Standards and Technology (NIST), editor: U.S. Department of Commerce: 2024.

Examples of Temporal Nature of AI Use Risk



Value Chain/ Component Integration

Non-transparent or untraceable integration of upstream components, including data that has been improperly obtained or not processed or other issues that diminish transparency or accountability for downstream users.

Data Privacy

Impacts due to leakage and unauthorized use, disclosure, or de-anonymization of biometric, health, location, or other personally identifiable information or sensitive data.

Harmful Bias or Homogenization

Amplification and exacerbation of historical, societal, and systemic biases

Confabulation

The production of confidently stated but erroneous or false content (known colloquially as "hallucinations" or "fabrications") by which users may be misled or deceived.

Intellectual Property

Eased production or replication of alleged copyrighted, trademarked, or licensed content without authorization (possibly in situations which do not fall under fair use); eased exposure of trade secrets; or plagiarism or illegal replication.

Information Security

Lowered barriers for offensive cyber capabilities; increased attack surface for targeted cyberattacks

Information Integrity

Lowered barrier to entry to generate and support the exchange and consumption of content which may not distinguish fact from opinion or fiction or acknowledge uncertainties. Loss of data providence

Human-AI Configuration

Interactions between a human and an AI system which can result in the human anthropomorphizing GAI systems or experiencing algorithmic aversion, automation bias, over-reliance, or emotional entanglement

Environmental Impacts

Impacts due to high compute resource utilisation in training or operating AI models, and related outcomes that may adversely impact ecosystems

Obscene, Dangerous or Abusive Content

Eased production of violent, inciting, radicalizing, threatening, obscene, degrading, and/or abusive imagery or content

CBRN Info or Capabilities

Eased access to or synthesis of materially nefarious information or design capabilities related to chemical, biological, radiological, or nuclear (CBRN) weapons or other dangerous materials or agents.

NB: These are a summary of the risks (with the addition of "research ethics" and "contractual") as described by United States government. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1). In: National Institute of Standards and Technology (NIST), editor.: U.S. Department of Commerce; 2024. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

Adding in research specific risks…

2.2 Protection of patient information

2.2.1 Respect the patient's right to know what information is held about them, their right to access their medical records and their right to have control over its use and disclosure, with limited exceptions.

2.2.2 Maintain the confidentiality of the patient's personal information including their medical records, disclosing their information to others only with the patient's express up-to-date consent or as required or authorised by law. This applies to both identified and de-identified patient data.

Australian Medical Association. Code of Ethics 2004. Editorially Revised 2006. Revised 2016. 17 March 2017.

Upstream Risks

Midstream/ Downstream Risks

Downstream Risks

Value Chain/ Component Integration

Non-transparent or untraceable integration of upstream components, including data that has been improperly obtained or not processed or other issues that diminish transparency or accountability for downstream users.

Research Ethics or Data Privacy

Participants have not provided their consent and/ or were not informed that their data would be analysed or used to train AI

Harmful Bias or Homogenization

Amplification and exacerbation of historical, societal, and systemic biases

Confabulation

The production of confidently stated but erroneous or false content (known colloquially as "hallucinations" or "fabrications") by which users may be misled or deceived.

Intellectual Property

Eased production or replication of alleged copyrighted, trademarked, or licensed content without authorization (possibly in situations which do not fall under fair use); eased exposure of trade secrets; or plagiarism or illegal replication.

Information Security

Lowered barriers for offensive cyber capabilities; increased attack surface for targeted cyberattacks

Contractual

AI is used in a manner that breaches the contracts entered by the University for their use

Information Integrity

Lowered barrier to entry to generate and support the exchange and consumption of content which may not distinguish fact from opinion or fiction or acknowledge uncertainties. Loss of data providence

Human-AI Configuration

Interactions between a human and an AI system which can result in the human anthropomorphizing GAI systems or experiencing algorithmic aversion, automation bias, over-reliance, or emotional entanglement

Environmental Impacts

Impacts due to high compute resource utilisation in training or operating AI models, and related outcomes that may adversely impact ecosystems

Obscene, Dangerous or Abusive Content

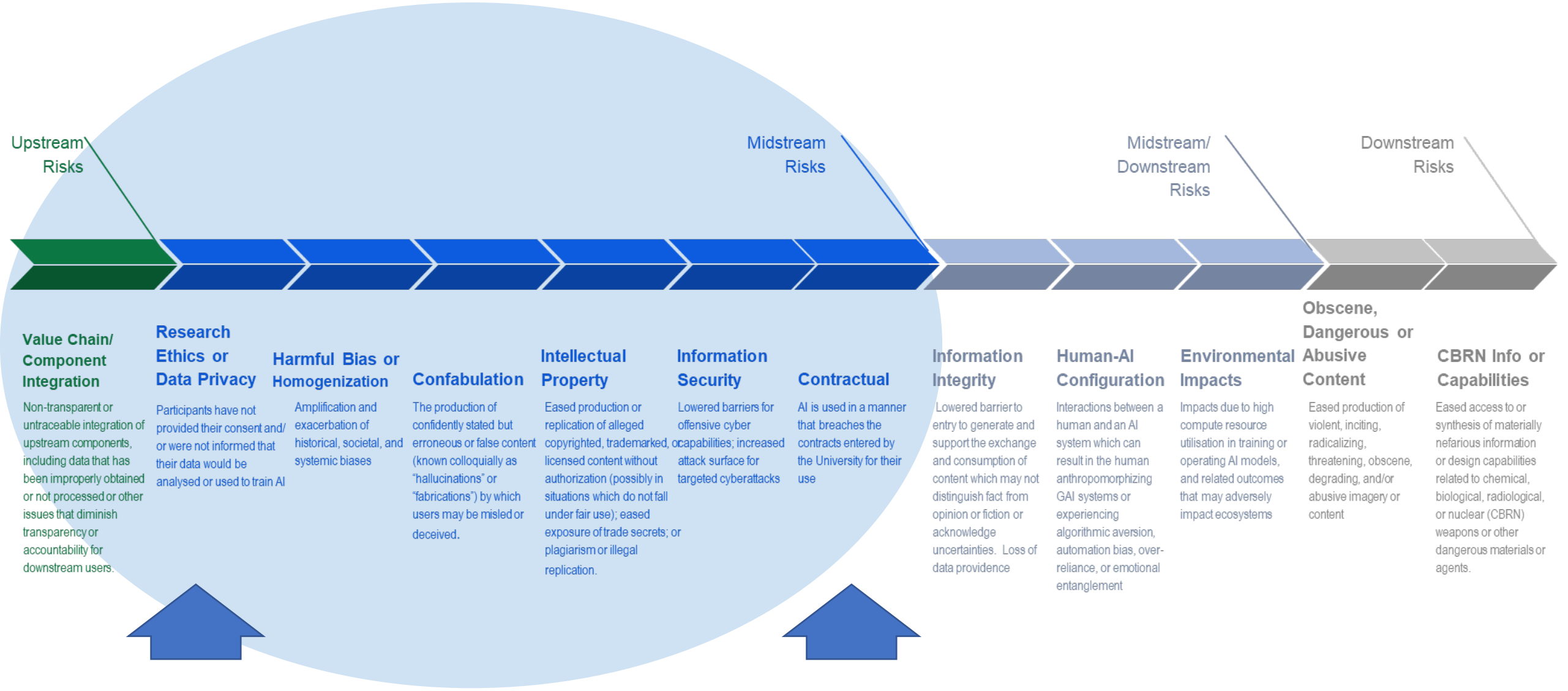
Eased production of violent, inciting, radicalizing, threatening, obscene, degrading, and/or abusive imagery or content

CBRN Info or Capabilities

Eased access to or synthesis of materially nefarious information or design capabilities related to chemical, biological, radiological, or nuclear (CBRN) weapons or other dangerous materials or agents.

NB: These are a summary of the risks (with the addition of "research ethics" and "contractual") as described by United States government. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1). In: National Institute of Standards and Technology (NIST), editor.: U.S. Department of Commerce; 2024. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

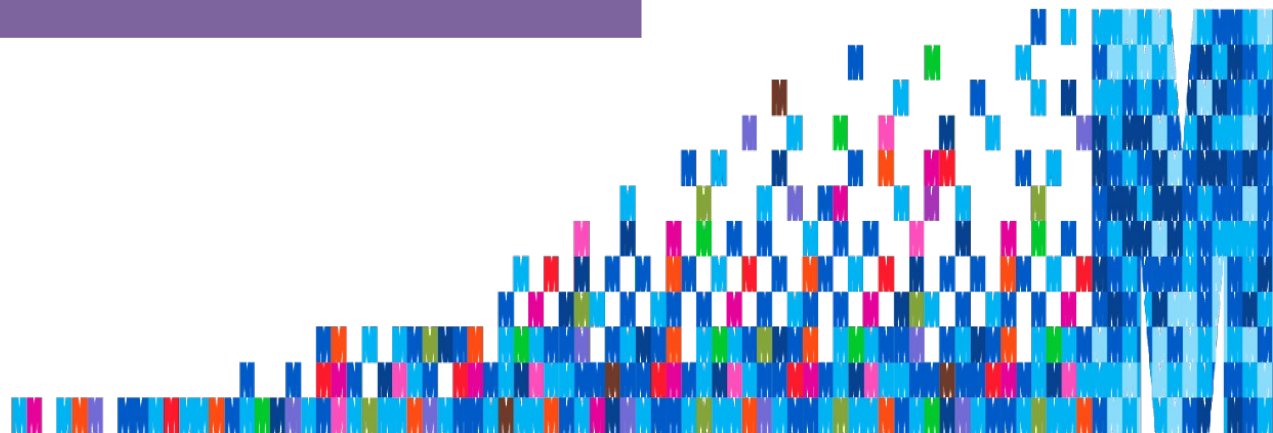
….then focussing on the key risks



NB: These are a summary of the risks (with the addition of "research ethics" and "contractual") as described by United States government. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1). In: National Institute of Standards and Technology (NIST), editor.: U.S. Department of Commerce; 2024. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

Lessons Learnt

- Cutting through the noise
- Finding the right people to work
- Integration
- The unexpected



MONASH University

Thank you

Acknowledgement: Komathy Padmanabhan

BoF: AI-Ready Research Data in Australia

Towards a Uni QLD Research Infrastructure AI Strategy

Bonno from UQ

UQ's Research Data

UQ holds 33 PB of research data (excl. backups).

10 years ago, UQ held 4.5 PB.

This amount is now growing by 10.5 PB annually.

This is an inhuman quantity of data.

All data-intensive disciplines will soon be reliant on inhuman quantities of data.

Responsible use of AI is the solution.

UQ’s Current (2025) Digital Research Infrastructure

High Performance Computing

Bunya supercomputer: 2,200 users, 14,000 CPU cores, 121 GPUs and 250 TB RAM.

Nectar Research Cloud

UQ runs Queensland’s Nectar Cloud: 36 servers + 35 GPUs for short-term use

Research Data Storage

80 PB total research storage + 19,500 active RDM users.

Trusted Research Environment (TRE)

Secure, isolated environment for sensitive data, Fives Safes Principles

Scientific Platforms and Portals

XNAT, IPP, Pitschi, RedCap, Galaxy, Australian Apollo Service, EMDPP, etc.

Containerised Compute Platform

On-demand compute for specialised research

Sovereign AI Capability

Made in Australia: Our AI Opportunity (ATSE report)

Rationale for pursuing AI sovereignty:

- National interest
- Lack of local customisation
- Narrowing tax base
- **Data misuse risks**
- **Interference risks**
- National **security risks**

Building Australia's AI Future – 5 key drivers:

- **Skilled workforce**
- Leading research
- **High-performance AI infrastructure**
- **Shared national datasets**
- Commercial pathways

UQ’s Sovereign AI Strategy: 3 Pillars

Curate

Our research data

The unique and novel data generated by researchers across our faculties and institutes is an essential strategic asset for UQ.

Core Platform: UQ RDM

(UQ Research Data Manager)

Co-design

Our embedded data science capability

Expert data scientists embedded within research teams and projects acting as a bridge between the research discipline/s and AI capabilities.

Core Platform: Data Science Collaborative Research Platform (Expertise CRP)

Compute

Our sovereign computational infrastructure

Global expertise and advanced infrastructure to leverage existing frameworks and big data assets to create new tools, reflective of the diversity of data UQ holds.

Core Platform: Research Computing Centre (Expertise and Infrastructure CRP)

UQ Research Data Manager - currently holding 33PB (not counting backups)

Curate

Our research data

The unique and novel data generated by researchers across our faculties and institutes is an essential strategic asset for UQ.

Core Platform: UQ RDM

(UQ Research Data Manager)

- **Centralised management:** Store, allocate, and access research data through one platform.
- **Flexible storage:** Multiple allocations per project (min. 1 TB, expandable).
- **Streamlined workflows:** Automatic provisioning on project approval.
- **Collaboration:** Simple sharing with UQ and external researchers.
- **Access options:** Desktop (UQ users) and cloud-based (UQ, external).
- **Compliance support:** Meets ethics, security, and funding (e.g. ARC) requirements.
- **Data protection:** Storage based on data-type sensitivity; backed-up and secure.
- **HDR support:** Integrated with thesis submission, review, and conferral workflows.

Research Data Management Policy and Procedure

Section 2 - Key Controls

(4) All UQ projects must be assigned an Information Steward (typically the Lead Chief Investigator of the project) at the outset of each research project. For undergraduate and postgraduate research projects, the Information Steward is the UQ Principal Advisor and cannot be the HDR candidate or student.

(5) At the outset of a research project, the Information Steward must ensure that a research data management plan is created in UQ Research Data Manager (UQRDM).

(6) The Information Steward is responsible for maintaining the research data management plan during the lifecycle of the project.

Section 3 - Process and Key Requirements

Stewardship and Control of Research Data

(7) Each project's Information Steward is responsible for ensuring that a research data management plan is in place at the start of a research project in UQRDM, and for reviewing and updating the plan as appropriate, giving consideration to such matters as:

a. Authority to make decisions on storage, retention, access, and publication of research data or records;
b. Requirements from funders, data providers (e.g. third-party data), research partners and collaborators;

Curate: Every project on UQ RDM (95%+ of all UQ Research) collects the following Metadata:

- Project name *
- Project description *
- Field of Research codes *
- Organisational unit *
- Project start date *
- Project end date *
- **Is this a HDR project? ***
- **Does this project use animal subjects? ***
- **Does this project use human subjects? ***
- **Will this project use or collect data not stored within UQRDM?**
- **Who owns any IP generated from this project**
- Animal ethics applications (lookup)
- **Human ethics** applications (lookup)
- Project owner *
- Project lead investigator *
- Other collaborators
- Services, for each:

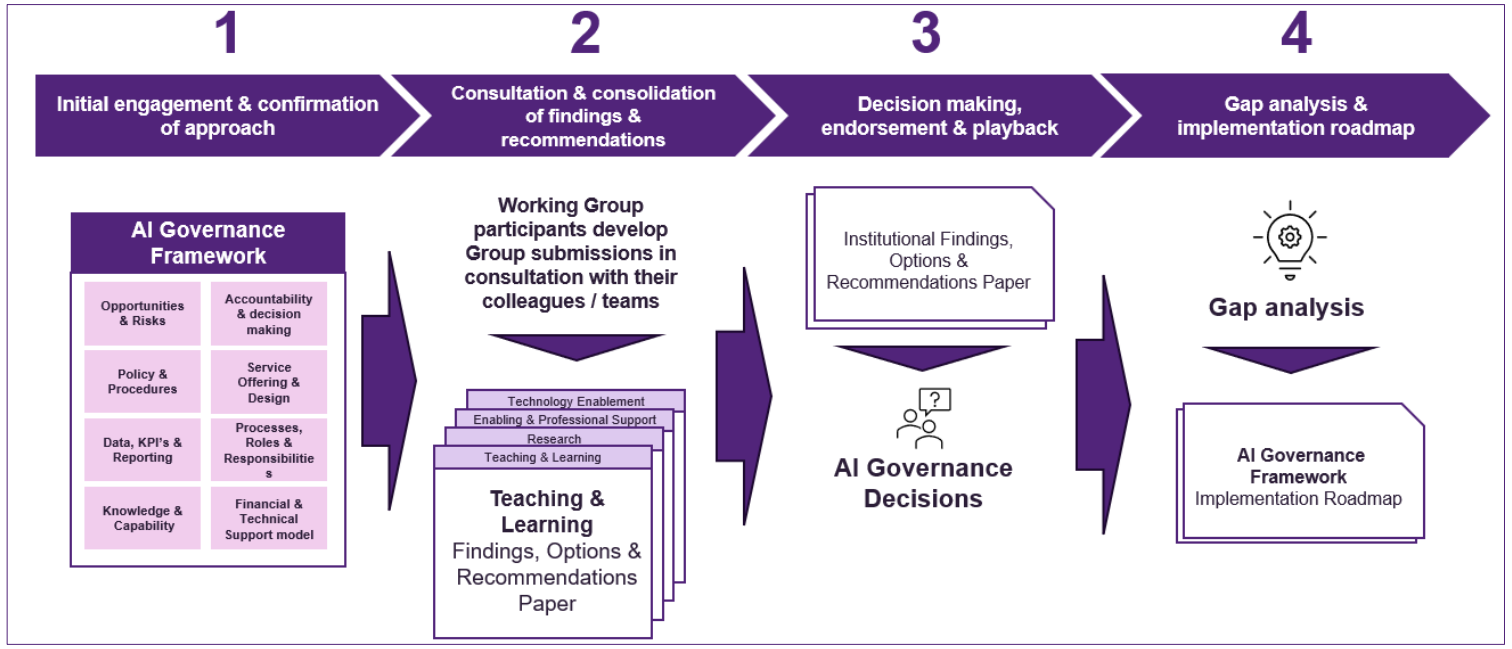
- **Storage:**
- Mandatory: **Storage label, Storage description, Type of data being stored**
- Optional: **Data retention, Has confidential information, Has human data**
- DRN:
- Mandatory: Label, notebook settings (vendor options)

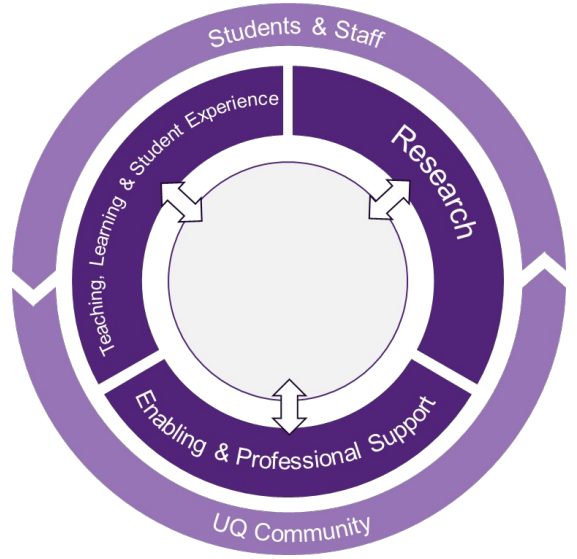
- **Human information collection from human beings via active participation ***
- **Research data generated through a clinical trial ***
- Data related to gene therapies *
- **Information of opinion about an identified individual**
- **Commercial in-confidence information ***
- **Sensitive ecological information ***
- Information on Security Sensitive Biological Agents

* = mandatory

UQ AI Governance Framework

Focus question	*How do we establish a scalable and repeatable approach for governing the adoption and use of AI by our Students and Staff?*





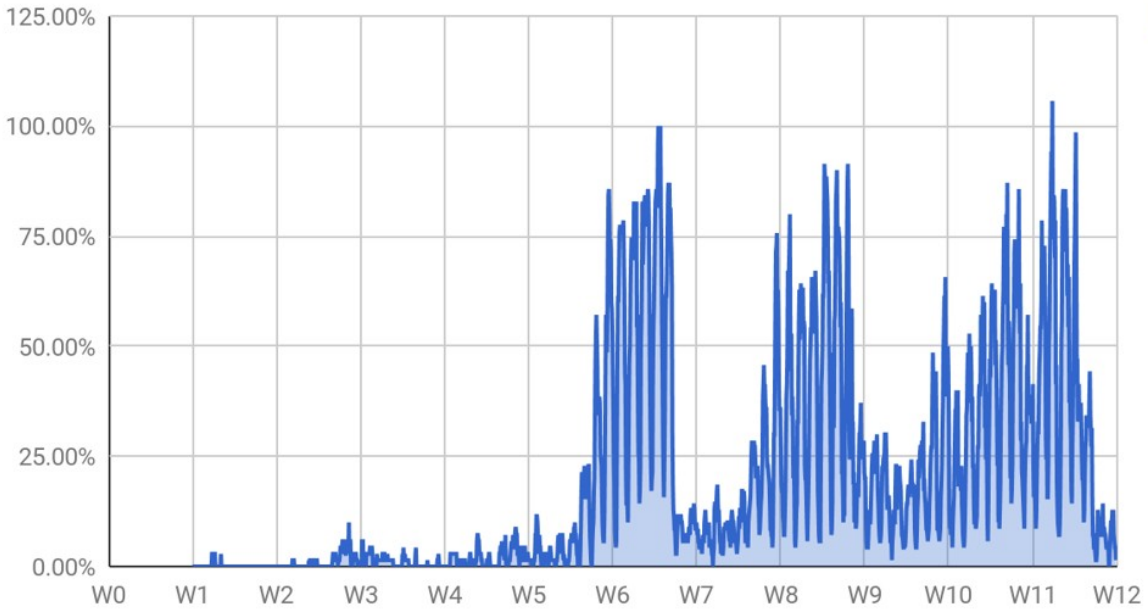
- Parallel project, COO portfolio
- Meeting with project Change Lead
- **Complimentary to this Research Infrastructure Strategy**
- Continue to meet regularly, to ensure alignment

AI: Teaching and Learning - UC San Diego slide

Coursework Activity Patterns

UCSD is on a quarter system with 10 weeks of instruction

Typical Quarter GPU Utilization (UCSD)



There will always be significant left over capacity for research.

Education must provision for peak demand.
Research mops up the left-overs.

UCSD operates a cluster with 132 GPUs dedicated to education

SDSC SAN DIEGO SUPERCOMPUTER CENTER

UC San Diego