Australian Research Data Commons

They are amongst us ...
Are Dataspaces already here?

ARDC Dataspaces program BoF Session,
eResearch Australasia 2025
23 October 2025

Australian Government | NCRIS National Research Infrastructure for Australia

ARDC is enabled by NCRIS

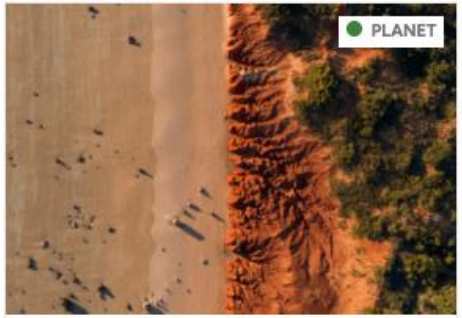
Australian Research Data Commons

Agenda

Segment	Time	Activity	Speaker
1	5	Intro to the Australian Dataspaces Program.	Kheeran/Shannon
2	10	Relevant Frameworks in overview. ● SAFE ● 5-SAFES ● IDSA RAM	Muhammad
3	15	Exemplar data sharing systems from a Dataspaces perspective. ● SEAF ● QCIF and KeyPoint	Amber Daniels Peter Marendy
4	25	Breakout Discussions: ● How do your systems compare against dataspaces? ● Commonalities and gaps	Everyone
6	5	● Next steps - join the community and let's keep working together. ● Wrap up.	Andy

Australian Research Data Commons

Intro to the Australian Dataspaces Program



Leveraging Dataspaces to Operationalise Data Sharing for a Shared Environmental Analytics Facility (SEAF)

Aligning the SEAF platform with the International Data Spaces (IDSA) Rulebook for secure, best-practice environmental...

Explore >

Biosecurity Dataspaces

Enabling trusted data sharing to reduce biosecurity risks for Australia

Explore >

Prototype Australian Dataspace Testbed Service

Enabling the testing and refinement of prototype dataspaces in Australia

Explore >

Dataspace Discriminator Checklist

Elements that distinguish dataspaces from other data sharing modalities

Seven distinguishing characteristics:

☐ 1. Distributed Peer-to-Peer Architecture

- Data remains at source (no mandatory central repository)
- Participants are equals, not client-server
- Connectors enable autonomous participation

☐ 2. Technical Data Sovereignty

- Providers retain control through technical enforcement
- Usage policies machine-readable (ODRL) and automatically executed
- Policy enforcement continues throughout data lifecycle

☐ 3. Trust Infrastructure

- Identity verification (certificates/credentials)
- Trust framework present (IDSA/Gaia-X/iSHARE/equivalent)
- Participant/component certification capability

☐ 4. Contract Negotiation Protocol

- Usage terms explicitly negotiated before access
- Standardised state machine (Request→Offer→Agreement)
- Contracts immutably stored by both parties

☐ 5. Standards-Based Interoperability

- DCAT catalogs + ODRL policies + Dataspace Protocol
- Open standards (W3C specifications mandatory)
- Federated architecture enabling cross-dataspace exchange

☐ 6. Federated Governance Capability

- Participation rules established and enforced
- Accountability framework with compliance monitoring
- Decision rights distributed (structure flexible)

☐ 7. Discovery & Observation

- Machine-readable metadata enabling automated finding
- Audit logging proportional to data sensitivity
- Monitoring capability for accountability

Consider all seven elements for consideration as a dataspace.

***Note:** Governance structure (centralised/federated/decentralised), trust framework choice, and technical implementation details are explicitly flexible*

Australian Research Data Commons

Frameworks Overview: How can they complement one another?

- Five Safes (TREs) ↔ IDSA Rule Book + RAM
- SAFE framework ↔ IDSA Rule Book + RAM

Alignment in Intent

Five Safes (TREs), IDSA Rule Book + RAM

Five Safes: Assessing risks associated with data sharing and release

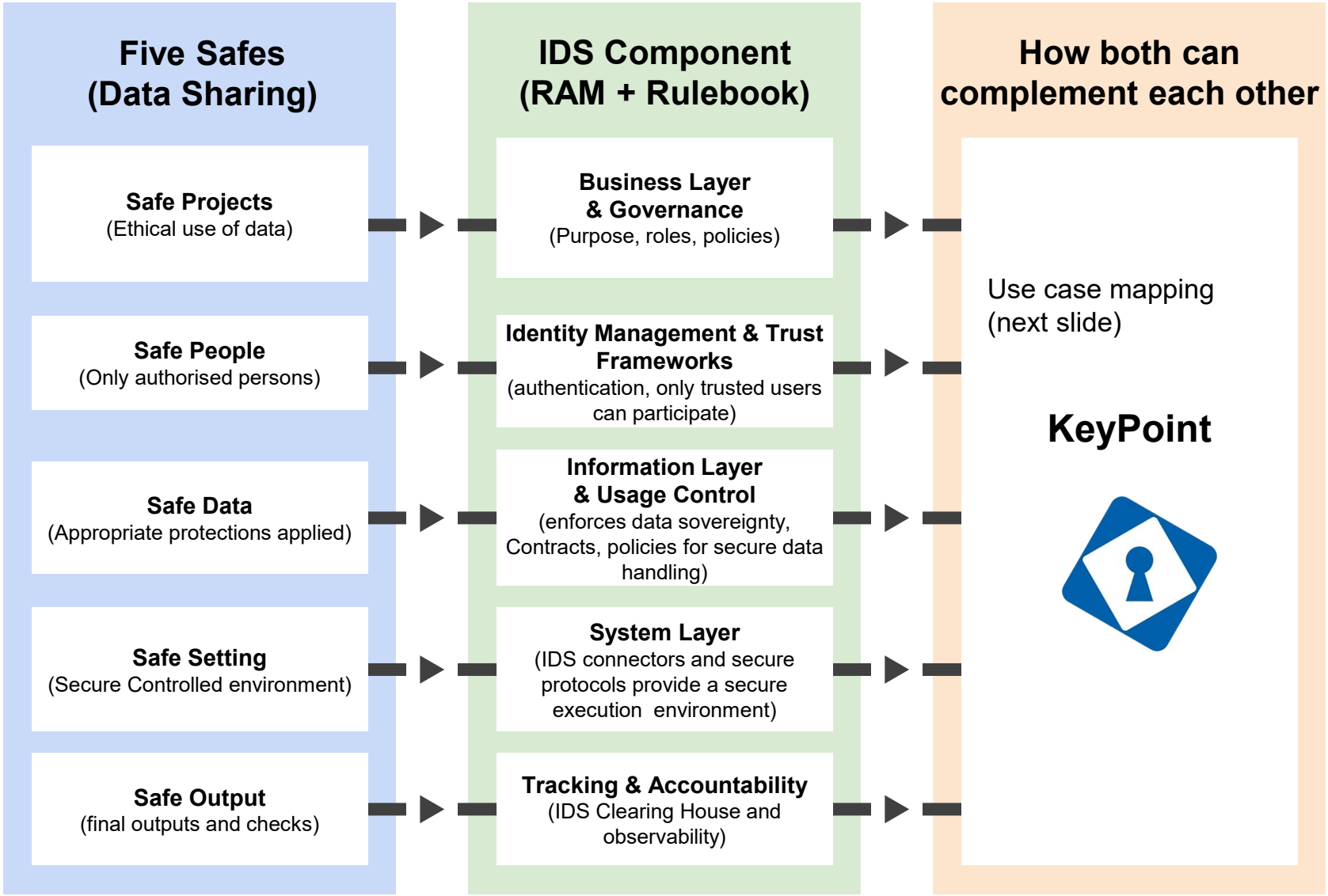
IDSA Rule Book: defines the legal, operational, functional, and technical rules for building and operating trusted data spaces

IDS RAM: translates the IDSA Rulebook into architecture and design specifications

Unified goal: enable **trusted, ethical, and secure data sharing** across platforms and sectors

Through the Five Safes and IDSA-RAM+Rulebook

Five Safes ↔ IDSA RAM Rulebook ↔ Complementary View



Use-case mapping (Keypoint)

Five Safes ↔ IDSA RAM+Rulebook ↔ Overlaps and enhancements

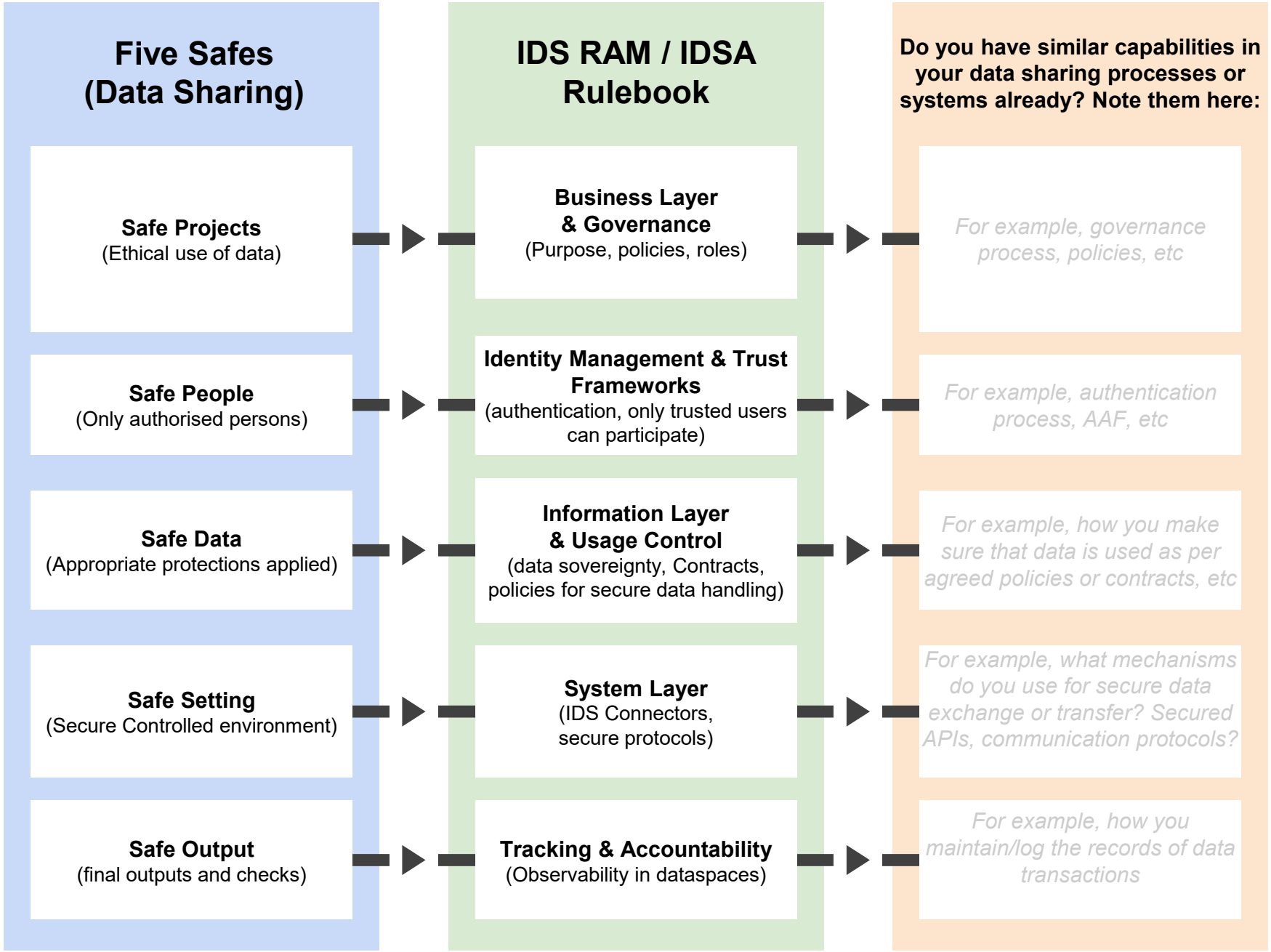
Layer	Five Safes Principle	KeyPoint (QCIF) Implementation	IDS (Rulebook+RAM) Reference	Overlaps & Identification (How dataspaces and TREs can complement each other)
Governance	**Safe Projects**	Strong governance model, though some elements of IDS would need to be done externally right now.	**Governance, Roles of participants in dataspace Rule 3.3 (Data Usage access Policies)**	Governance processes from Dataspaces could be integrated into the user access and roles within a TRE.
Identity & Trust	**Safe People**	Use of institutional identity via AAF. Multi-stage process to grant access.	**Establishing_trust.md Identity Management & Trust Frameworks**	TREs would need to incorporate the dynamic attributes from dataspaces. This is important for frameworks such as CARE Principles. This may come from external IdP registries.
Data Sovereignty	**Safe Data**	Moderated ingress and egress gateways. Governance model allows authorised delegates to enforce data owner policies.	**Policy_Enforcement.md Information Layer & Usage Control**	Use of dataspace defined rules within a TRE could inform data access for users. This could be provisioned in a hybrid manner with some aspects automated and others requiring manual enforcement.
Access & Environment	**Safe Settings**	Role Based Access Controls to secure internet isolated analysis environment.	**3.5 System layer Connector, Secure Execution Environment**	TREs offer a controlled secure environment for approved users to access the data.
Output Control	**Safe Outputs**	Moderated egress process conducted within the secure environment.	**Usage tracking and enforcement**	TREs allow usage of the data to be controlled in alignment with data owner requirements.

Australian Research Data Commons

Does Your Data Sharing Fit Here?

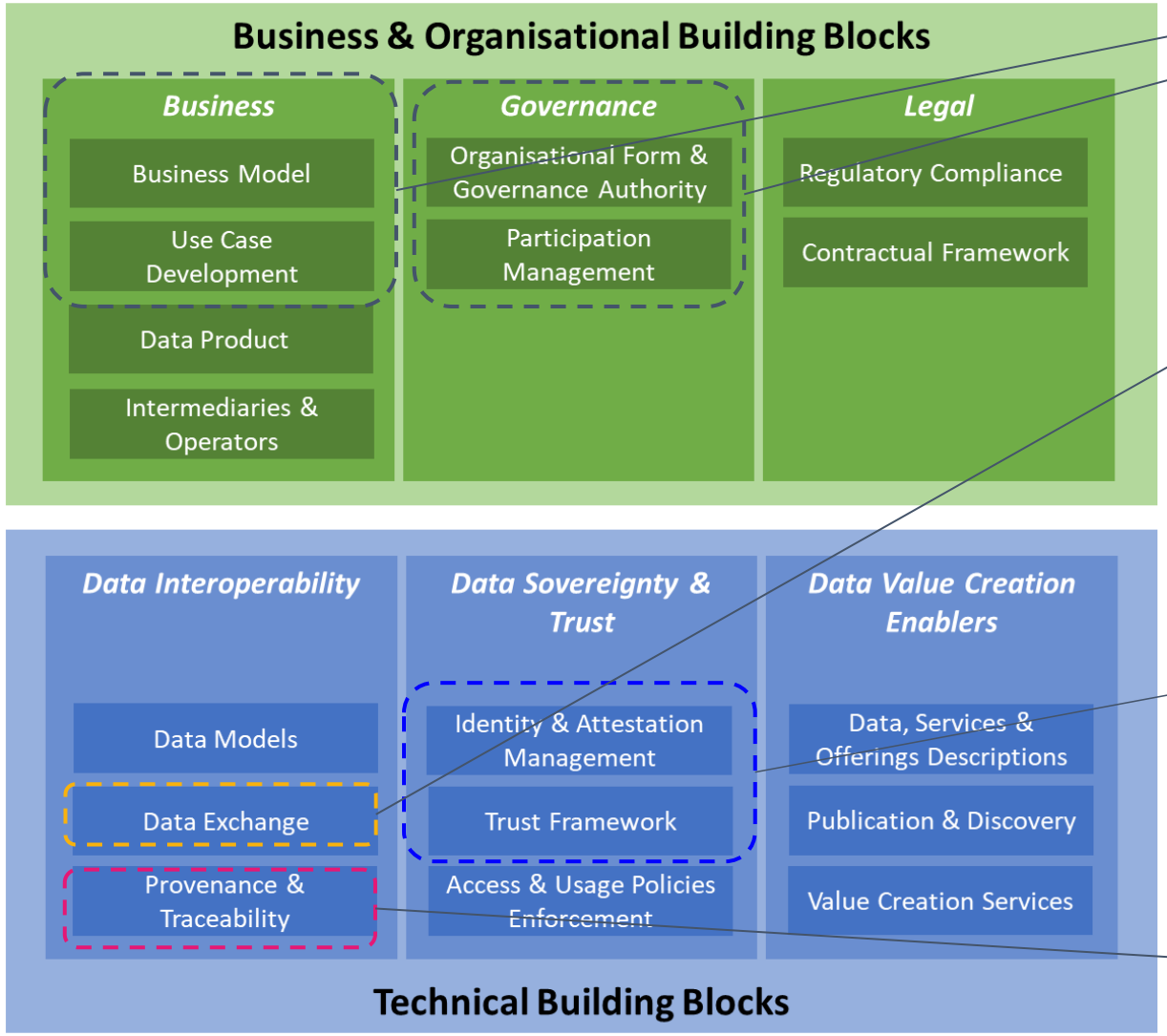
This figure shows how the Five Safes framework aligns with IDS RAM and IDSA Rulebook principles.

- Do your data sharing processes or systems address any of these requirements?
- Could they be enhanced by any of them?



Through the lens of DSSC building blocks

The Data Spaces Support Centre (DSSC) supports the deployment of the common European data spaces



Safe Projects → Business Layer & Governance

- DSSC Blueprint:
  - **Business Model**
  - **Use Case Development**
  - **Organisational Form & Governance Authority**

Safe Setting → System Layer

- DSSC Blueprint:
  - **Data Exchange (connectors)**
  - **Secure protocols (DSP)**

Safe People → Identity Management & Trust Frameworks

- DSSC Blueprint:
  - **Identity & Attestation Management**
  - **Trust Framework**

Safe Output → Auditing, Tracking & Accountability

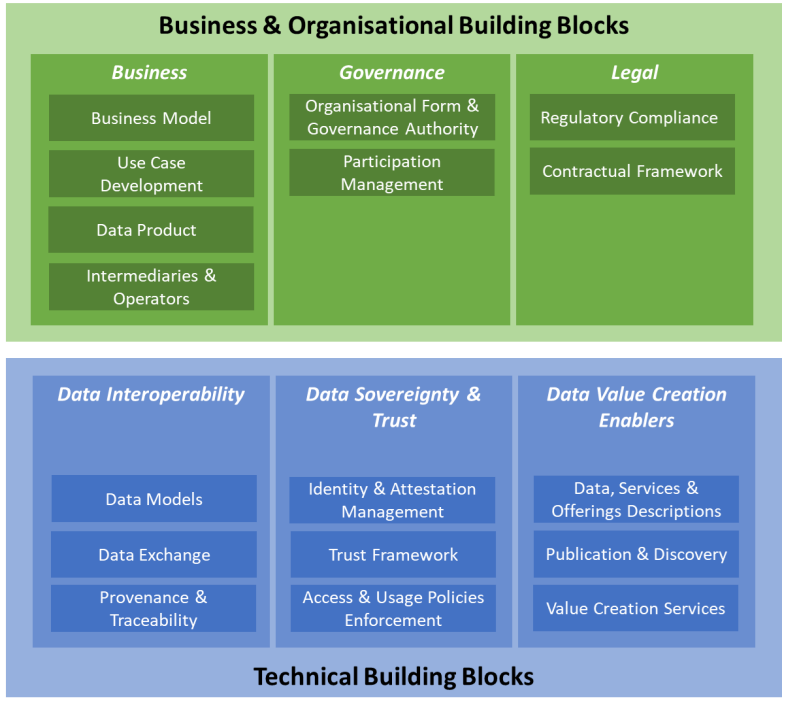
- DSSC Blueprint:
  - **Provenance & Traceability**
  - **Participation Management**

Australian Research Data Commons

Compare your current architecture (Phase 2 Shaping of Dataspaces)

What trust frameworks do you use for data sharing?

- Identity and access management such as AAF?
- Policy enforcement mechanisms?
- Governance model and policies and data sharing agreements?
- Data exchange mechanisms such as API data transfer?
- How to you track the data transactions (Provenance and traceability)?



Safe Framework to the IDS-RAM

The Shared Analytic Framework For The Environment (SAFE 2.0) : https://wabsi.org.au/category/publications/

SAFE Framework ↔ IDSA Rulebook/Architecture

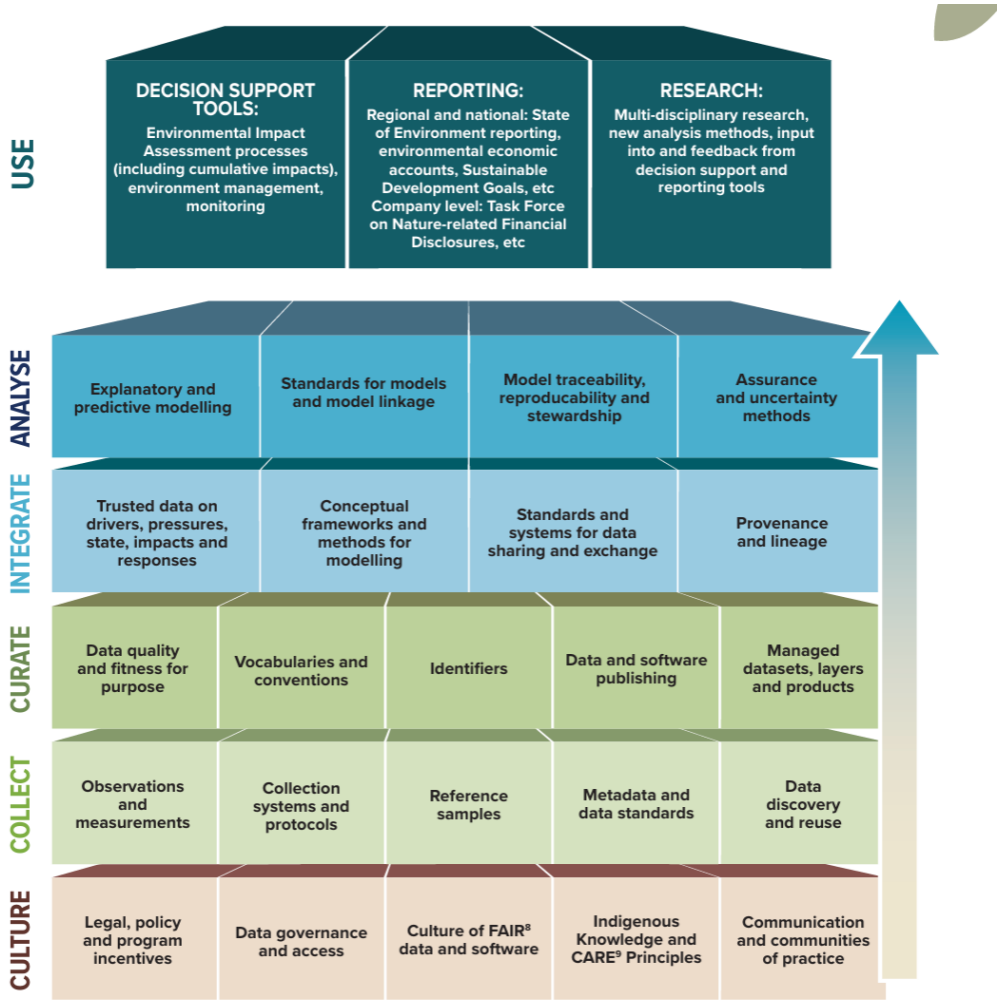


FIGURE 3: SAFE – Layers and capabilities

<--- READ RIGHT TO LEFT

Description	RAM Requirement	RAM Requirement Category	RAM Layer
Basic and business roles	Roles		**Business layer**
	Role interactions		
CA, DAPS, ParIS	Identities		
	Usage contracts		
	Roles	Trust	**Functional layer**
Connector certification	Identity management		
User certification	User certification		
Connector X509 certs	AuthNZ	Security and data sovereignty	
	Usage policies and enforcement		
Encryption	Trustworthy communication		
	Security by design		
IDSA certification processes	Technical certification		
	Data source description	Ecosystem of data	
	Brokering		
	Vocabularies		
IDSA connector	Operation	Standardised interoperability	
IDSA connector	Data exchange		
	Data processing and transformation	Value-adding apps	
	Data app implementation		
	Providing data apps		
	Installing and supporting data apps		
	Clearing and billing	Data markets	
	Usage restrictions and governance		
	Legal aspects		

Australian Research Data Commons

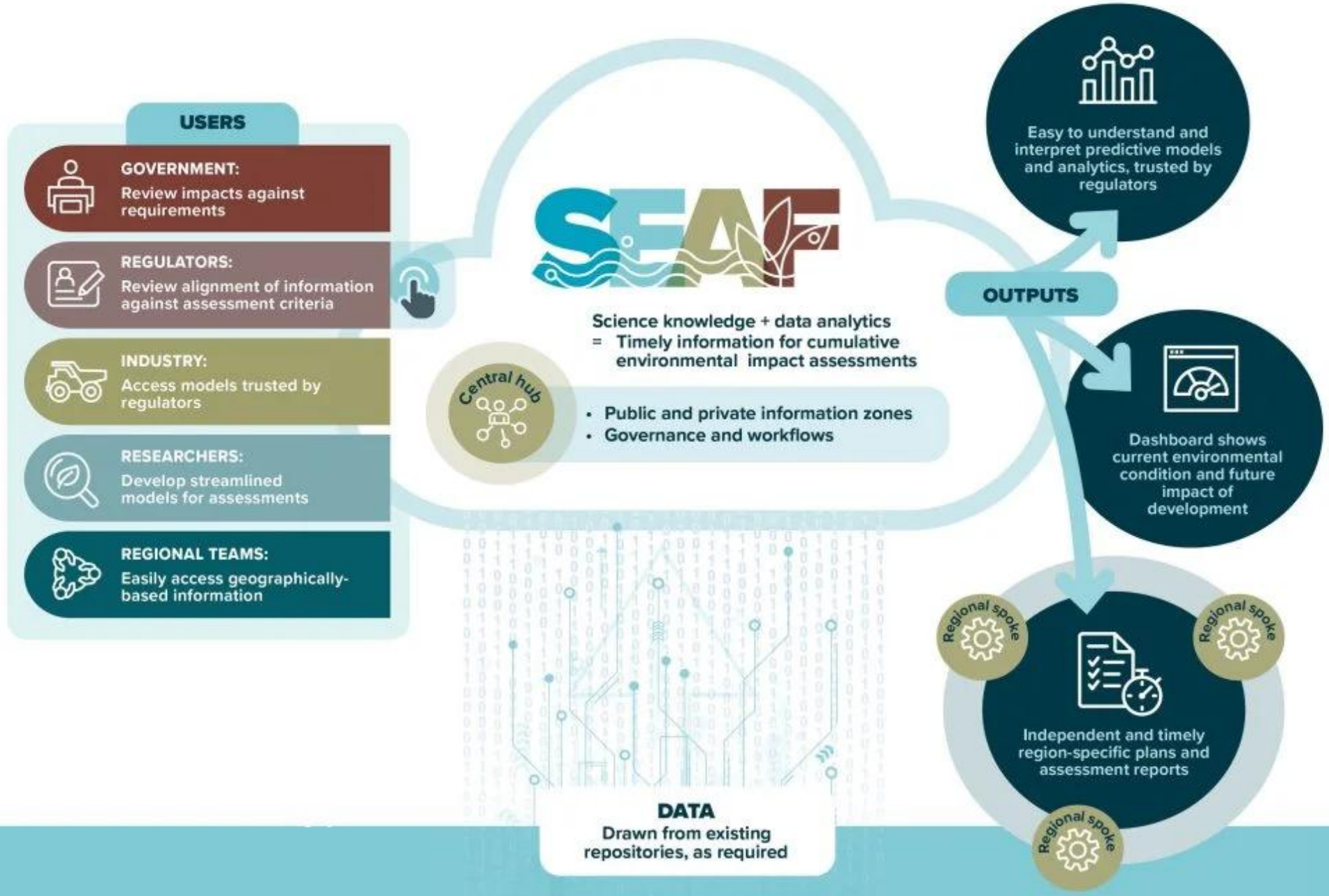
Data sharing systems from a Dataspaces perspective.

Exemplar 1:

- *SEAF Governance Models and Frameworks*
- *Amber Daniels, WA Biodiversity Science Institute*

SEAF
Governance Models and Frameworks

A SHARED ENVIRONMENTAL ANALYTICS FACILITY (SEAF)


USERS
GOVERNMENT:
Review impacts against requirements
REGULATORS:
Review alignment of information against assessment criteria
INDUSTRY:
Access models trusted by regulators
RESEARCHERS:
Develop streamlined models for assessments
REGIONAL TEAMS:
Easily access geographically-based information
SEAF
Science knowledge + data analytics
= Timely information for cumulative environmental impact assessments
Central hub
• Public and private information zones
• Governance and workflows
DATA
Drawn from existing repositories, as required
OUTPUTS
Easy to understand and interpret predictive models and analytics, trusted by regulators
Dashboard shows current environmental condition and future impact of development
Regional spoke
Regional spoke
Regional spoke
Independent and timely region-specific plans and assessment reports

Governance Complexity

SEAF is expanding

- Pilbara Groundwater (industry, research, government)
- Cockburn Sound (marine research, port authorities, industry)
- Additional Spokes and use cases in the pipeline across AU

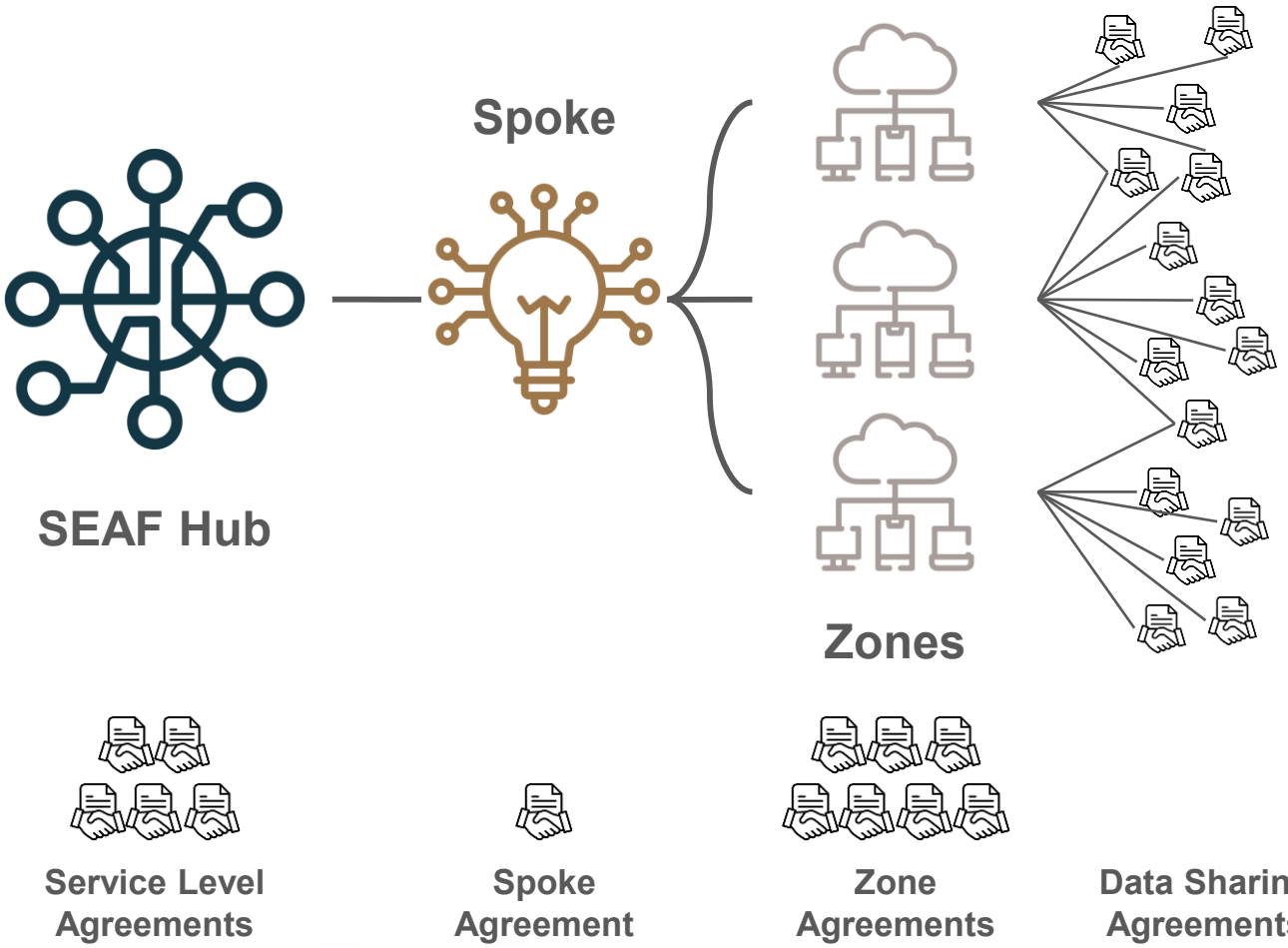
Each new partnership triggers new contracts

- Partnership contracts (Spoke Agreement accession), bilateral and multilateral agreements
- Zone Agreements (creation of bespoke secure analytics environments
- Data Sharing Agreements to furnish Zones (bilateral, multilateral; with SEAF, with SEAF and others)

Potential Risks

- Governance complexity can multiply with each new partnership
- Inconsistent implementation of standards across agreements and operations
- **How do we scale while maintaining quality, sustainability and robustness?**

SEAF Hub and Spokes



- Each layer needs consistent governance
- Custom agreements generate unsustainable overhead
- Risk implementing different standards across identical issues
- **How do we scale without reinventing governance and technology for each layer?**

Metagovernance

DSSC Blueprint
IDSA Rulebook

What a dataspace is and how it should work

Methodology

Sitra Rulebook

Business architecture, good governance & ethics

Implementation

SEAF Org Governance
SEAF Data Governance
Legal Agreements
Technical Standards

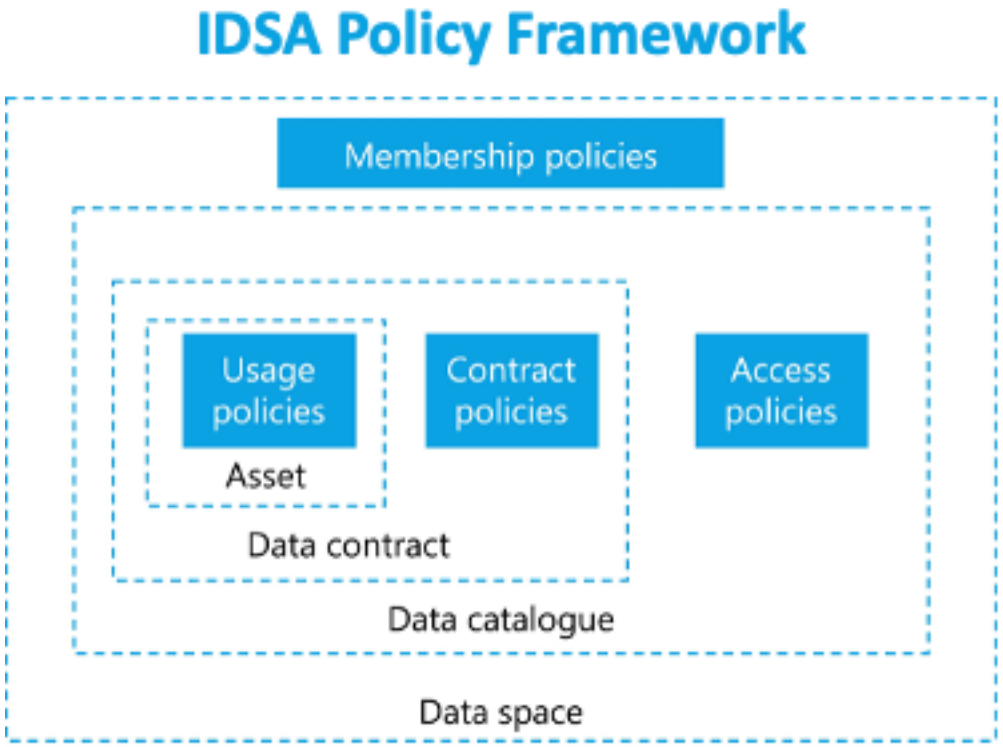
Regulatory Environment

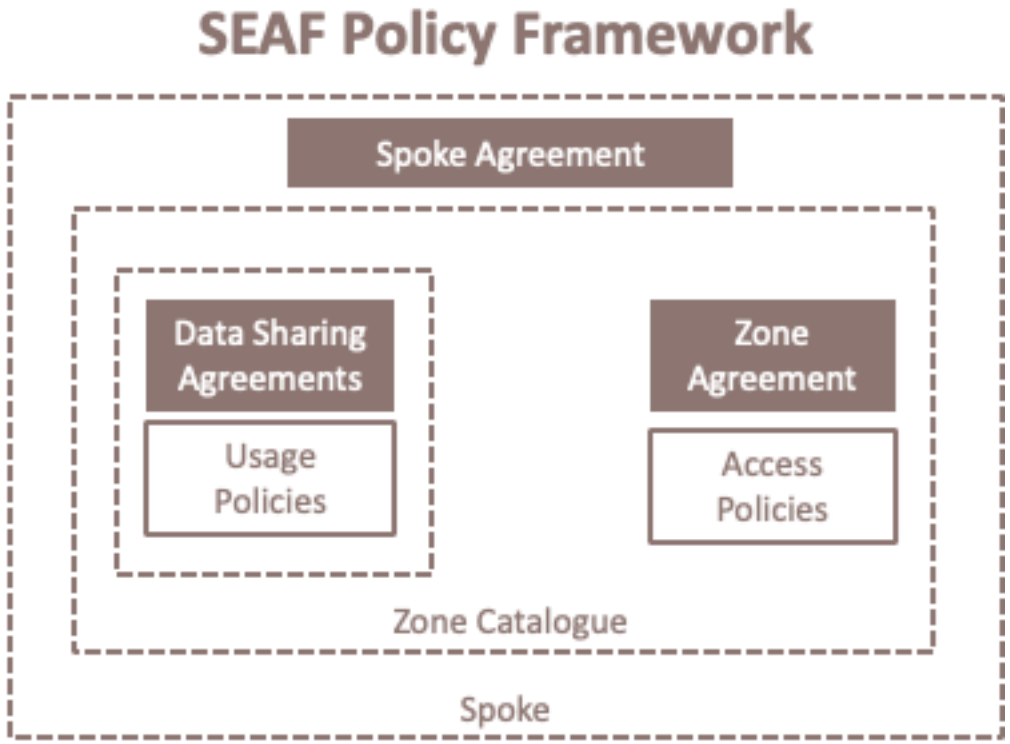
State and Commonwealth legislation governing
privacy, security, sovereignty, environment, cultural heritage, and more...

Mapping Frameworks to Implementation

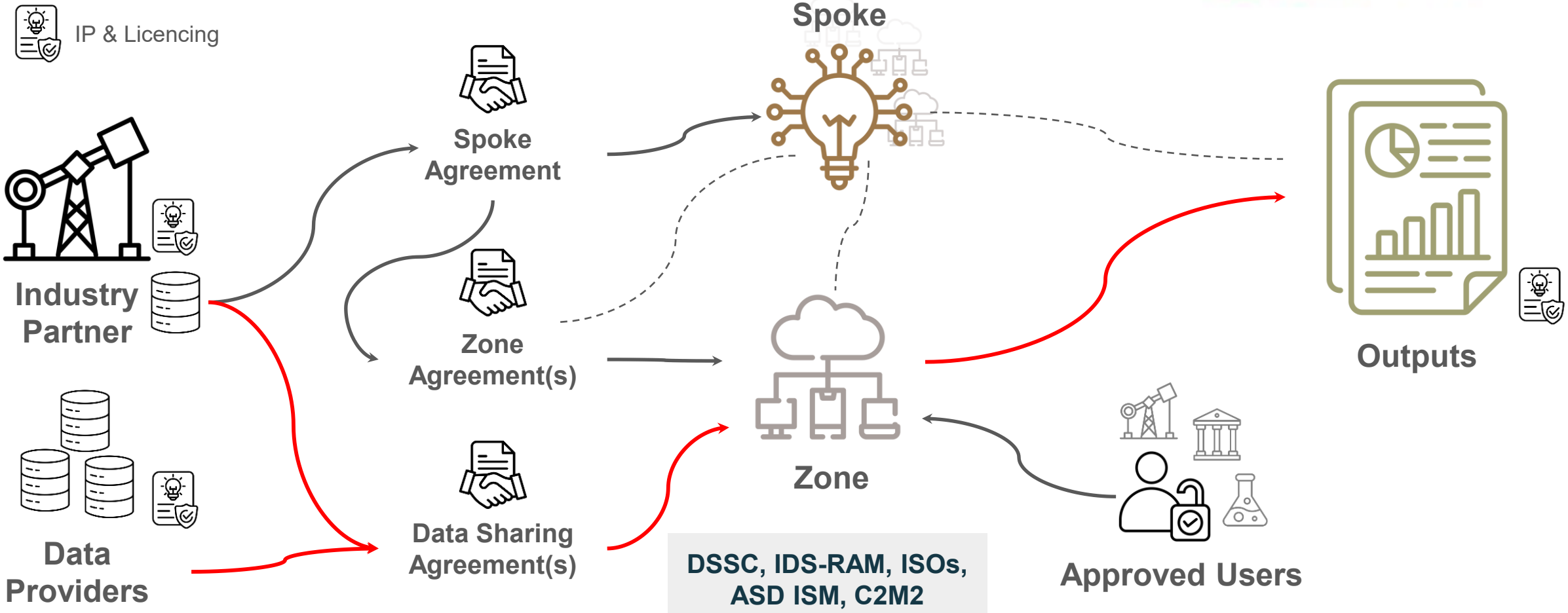
Framework	Purpose	SEAF
SAFE 2.0 Shared Analytic Framework for the Environment	National environmental data supply chain framework	SEAF operational model and quality control mechanism
DSSC, IDSA, Sitra Rulebooks	Dataspace architecture & business framing methodology	Hub-Spoke Model Spoke → Zone → DSA structure
ASD ISM, ACSC E8, ISO27001, C2M2, AARC BPA / AAF PDK	Security baselines, management, and capability (maturity) assessments; identity federation patterns	Cybersecurity Policy & Standards Security Incident Response Procedure Data governance standards
Five Safes	Data access control	Zone configuration and operation

Policy Framework Alignment





Operational Data Flow →



What we are learning

What makes sense

- Framework mapping reduces governance overhead
- Bridging conceptual frameworks to actionable methodologies

Challenges

- Interpretation of metagovernance for specific domains and jurisdictions
- Australian regulatory mappings need real translation
- Environmental domain specificity requires framework customisation

What is useful

- Three-level approach:
  → Metagovernance
  → Methodology
  → Implementation
- Mapping AU security frameworks to dataspaces frameworks, especially when working with government and highly regulated industry
- Sharing our experiences

Thank you

amber.daniels@wabsi.org.au

A SHARED ENVIRONMENTAL ANALYTICS FACILITY (SEAF)

Australian Research Data Commons

Data sharing systems from a Dataspaces perspective.

Exemplar 2:

- *QCIF KeyPoint*
- *Peter Marendy and Stephen Bird, QCIF*

Australian Research Data Commons

QCIF Digital Research³

KeyPoint - A secure collaborative research environment

Data custodian governed

Fine-grained access controls and permissions
Highly governed environment
File in and file out approval processes

Secure remote access from anywhere

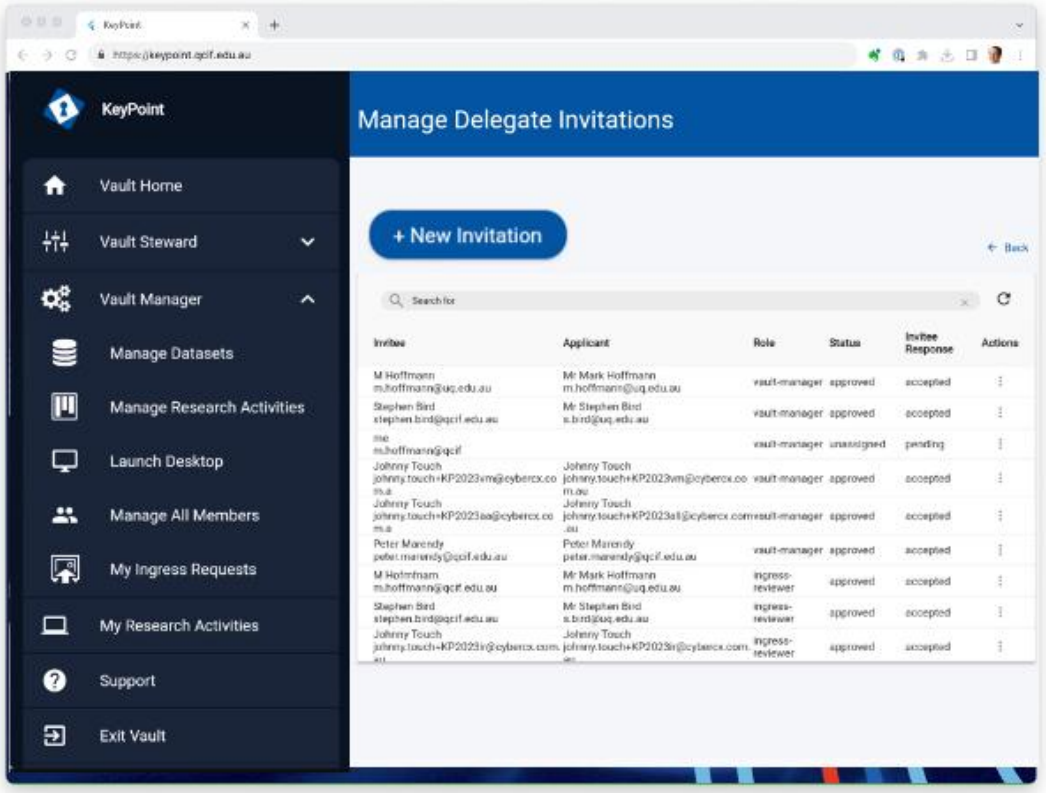
Restricted access (even internally)
Remote desktop access
No printing, copy/paste, or access to internet/email

Pre-installed suite of software available

Customisable to the project and user
Office/Excel, STATA, R, Python, SPSS and SAS (incurs additional cost)
Ability to request R/Python packages

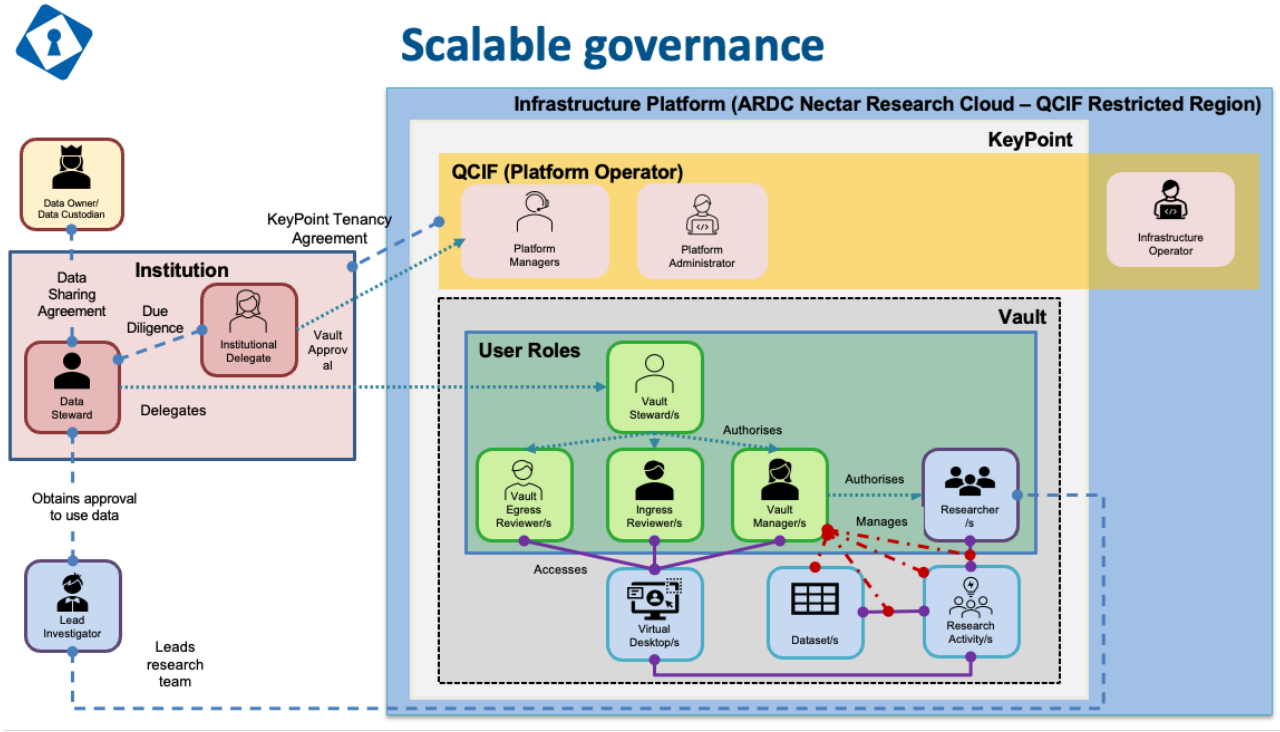
High-powered computing

Various flavours Windows Virtual Machines (VDI) (Can be customised)
High memory and GPU nodes



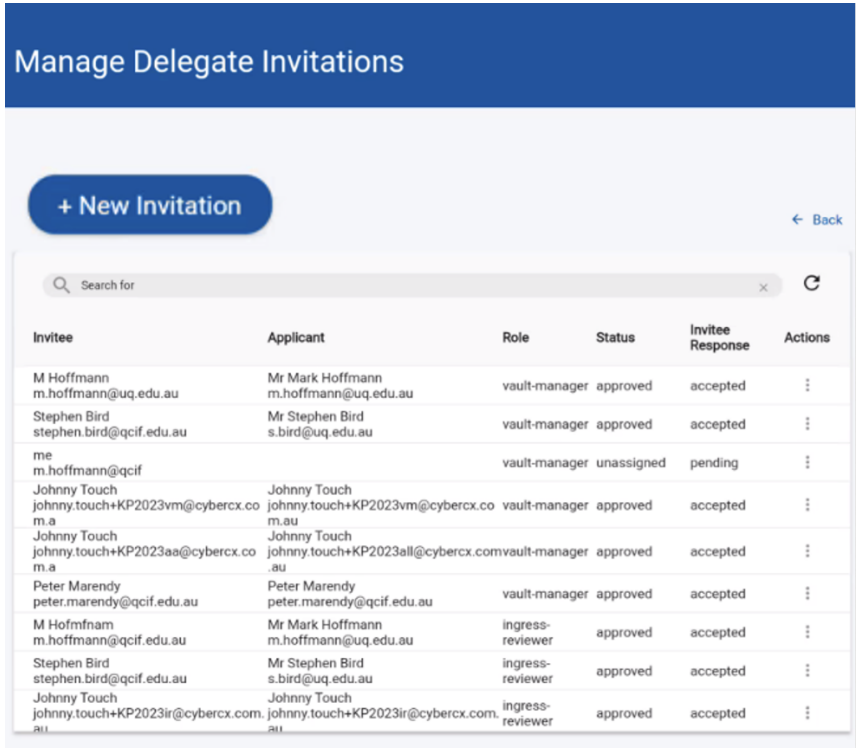
Safe Projects

- KeyPoint enforces a governance model with defined roles and capabilities for those roles
- Agreements with a Data Owner occur externally to KeyPoint, but there is an assertion made by the person/org bringing data into KeyPoint that they have the right to use it in the environment and will comply with requirements from the Data Owner



Safe People

- On-boarding process that includes awareness training for use of sensitive data before being enabled for KeyPoint
- Being enabled for KeyPoint does not grant you access, you need to be invited in to a Vault and Role and optionally a Research Activity
- Use Australian Access Federation to be able to use institutional IdPs for authentication (can leverage future AAF Trust and Identity programs)
- Add our own MFA challenge
- Multi-step invitation process to grant access with opportunity to decline, rescind
- Access can be suspended (re-instated) and revoked
- Strong role-based access controls



Australian Research Data Commons

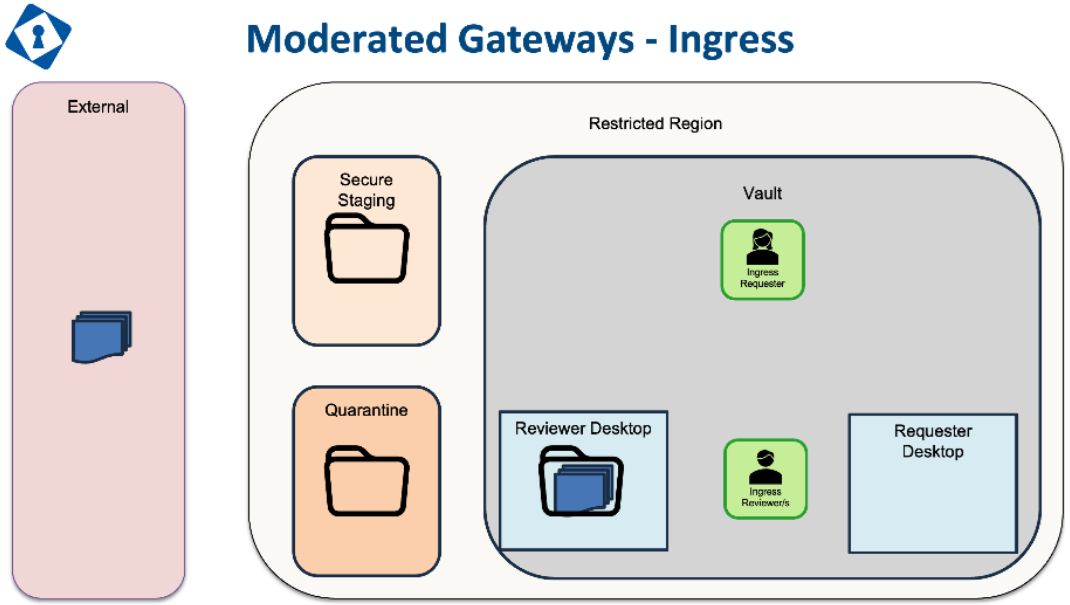
QCIF Digital Research³

Safe Data

- Governance is handed over to the owners of the Vault
- Part of their role is to enforce the requirements of the Data Owner, which includes what the data is used for

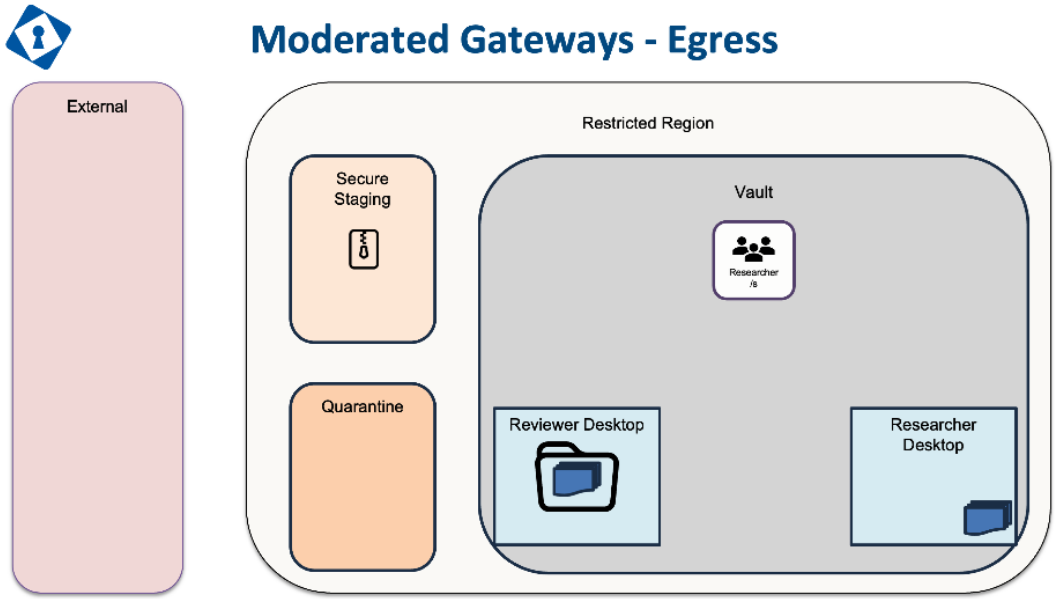
Safe Settings

- Mediated data ingress and egress, all performed read-only inside the environment
- Ingressed data is automatically scanned for malware
- Data access and analysis occurs on secure internet isolated virtual desktops
- One user on a desktop at a time
- Uses roaming profiles so no data stored locally on desktops
- Strong role-based access control to enforce strict project separation
- All data stored encrypted at rest
- Collaboration spaces in research activities
- Runs in a restricted region of the Nectar Research Cloud



Safe Settings

- Easily connect and disconnect datasets to/from research activities
  - a dataset can be shared to 1 or more research activities
  - researchers only see data connected to their current research activity, even if they are a member of multiple research activities
- All external traffic to the environment is encrypted
- All actions are logged in an audit trail



Australian Research Data Commons

QCIF Digital Research

Safe Outputs

- Governance is within the remit of the Vault Steward and their delegate Egress Reviewer(s)
- Multi-step process to egress data
- All data being egressed undergoes a review by an Egress Reviewer
- The Egress Reviewer can inspect data in read-only mode on a virtual desktop inside the environment
- Only approved data is able to be downloaded from the environment

Australian Research Data Commons

Use-case mapping (Keypoint)

From the Five safes / IDS Rulebook+RAM perspective

Layer	Five Safes Principle	KeyPoint (QCIF) Implementation	IDS (Rulebook+RAM) Reference	Overlaps & Identification (How dataspaces and TREs can complement each other)
Governance	Safe Projects	Strong governance model, though some elements of IDS would need to be done externally right now.	Governance, Roles of participants in dataspace Rule 3.3 (Data Usage access Policies)	Governance processes from Dataspaces could be integrated into the user access and roles within a TRE.
Identity & Trust	Safe People	Use of institutional identity via AAF. Multi-stage process to grant access.	Establishing_trust.md Identity Management & Trust Frameworks	TREs would need to incorporate the dynamic attributes from dataspaces. This is important for frameworks such as CARE Principles. This may come from external IdP registries.
Data Sovereignty	Safe Data	Moderated ingress and egress gateways. Governance model allows authorised delegates to enforce data owner policies.	Policy_Enforcement.md Information Layer & Usage Control	Use of dataspace defined rules within a TRE could inform data access for users. This could be provisioned in a hybrid manner with some aspects automated and others requiring manual enforcement.
Access & Environment	Safe Settings	Role Based Access Controls to secure internet isolated analysis environment.	3.5 System layer Connector, Secure Execution Environment	TREs offer a controlled secure environment for approved users to access the data.
Output Control	Safe Outputs	Moderated egress process conducted within the secure environment.	Usage tracking and enforcement	TREs allow usage of the data to be controlled in alignment with data owner requirements.

Australian Research Data Commons

Breakout Discussions

- Individually (5 mins)
  - Consider your own data sharing:
    - How do your systems and processes compare against the dataspace model?
    - Where could dataspace ideas help?

- Team up (15 mins)
  - Discuss and compare notes.

- Come together (5 mins)
  - Commonalities and gaps?
  - Shared themes?

Australian Research Data Commons

Breakout Discussions

- Key Takeaways:

Want to know more?

Australian Dataspaces Program
https://ardc.edu.au/program/australian-dataspaces/

Australian Dataspaces: An Introduction and FAQs
https://ardc.edu.au/resource/australian-dataspaces-an-introduction-and-faqs/

Australian Dataspaces Community Site
https://sites.google.com/ardc.edu.au/australian-dataspaces/home

STAY IN TOUCH

Australian Dataspaces

Establishing dataspaces to create trusted, secure ecosystems for secure data exchange between research, industry and government in Australia

Register your interest

https://ardc.edu.au/program/australian-dataspaces/

https://sites.google.com/ardc.edu.au/australian-dataspaces/implementers-network

Australian Research Data Commons

CONTACT

ardc.edu.au

contact@ardc.edu.au

+61 3 9902 0585

Australian-Research-Data-Commons

Subscribe
https://ardc.edu.au/subscribe