Delivering a secure, trusted and scalable infrastructure environment for data governance, control and management of sensitive data for remote analysis for the Australian landscape.

Mat Ishac[1], Stephen Bird[2],

[1]*Monash University, Melbourne, VIC, Australia*

[2]*Queensland Cyber Infrastructure Foundation, QLD, Australia*

Australian Research Data Commons

Australian National University

MONASH University

QCIF

Swansea University Prifysgol Abertawe

saxinstitute

UNSW SYDNEY

Curtin University

Acknowledgement of Country

We begin this presentation by acknowledging the Jagera and Turrbal people as the Traditional Custodians of Meanjin, where we gather here today, and pay our respects to their Elders past, present and emerging.

Agenda

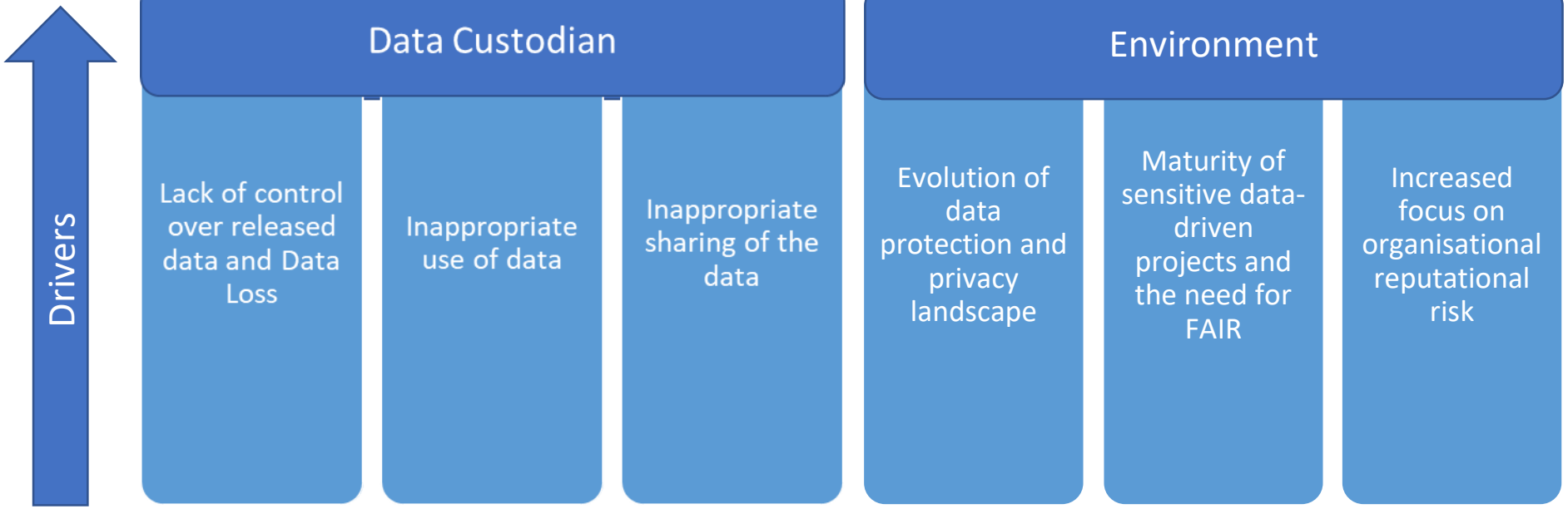
- **The Need for Secure eResearch Platforms**
- **Platforms Summary**
- **The Five Safes**
- **Project Approach**
  - Research Infrastructure CoP
  - Technical Working Group
  - ARDC/Nectar Restricted Region
- **Exemplar Projects**
- **Additional project delivery**
- **Into the future**
- **Q&A**

The Need

Sensitive Data Collaboration

Data custodians require a robust and secure environment to **manage** data

Researchers require a simple and secure interface to **access** and **analyse** data



Monash SeRP

A secure eResearch platform for researchers to share and store their data in a secure, scalable and sensitive approach

Monash Secure eResearch Platform (SeRP) is a secure environment for sharing research data for collaboration and analysis, within the control and governance of the data custodian. Monash SeRP allows the Data custodian or the delegated project manager (Data Custodian) to have visibility and control over how their data is being used by other approved researchers.

- Scalable data governance
- Simple User Interface.
- Data Linkage Module
- Full suite of analytical tools
- Store and analyse diverse forms of data.
- Large scale High Performance Computing capability.
- Secure, remote access

MONASH University

Swansea University
Prifysgol Abertawe

QCIF

KeyPoint

- Purpose-built environment for the remote analysis of sensitive data
- Hosted in a restricted region of the Nectar Research Cloud
- Scalable governance model that puts you in control of your data
- Leverages AAF for authentication, so you can use your home institution’s credentials
- Not restricted to population-health data sets - can be used for sensitive data from all research domains
- Enforces strict project separation at the Virtual Desktop
- Flexibility to provide various sizes of Virtual Desktops, including Large Memory and NVIDIA A40 GPUs, along with customisable software stacks (comes with a range of applications including SAS, Stata, SPSS)
- National finalist in iAwards

The Five Safes

National statistical offices (NSOs) **5 safes framework** manage the disclosure risk for releasing data

5 safes principles are to balance safe projects, people, settings, data and output against disclosure risk and utility

Approach: Research Infrastructure CoP

- Community Engagement

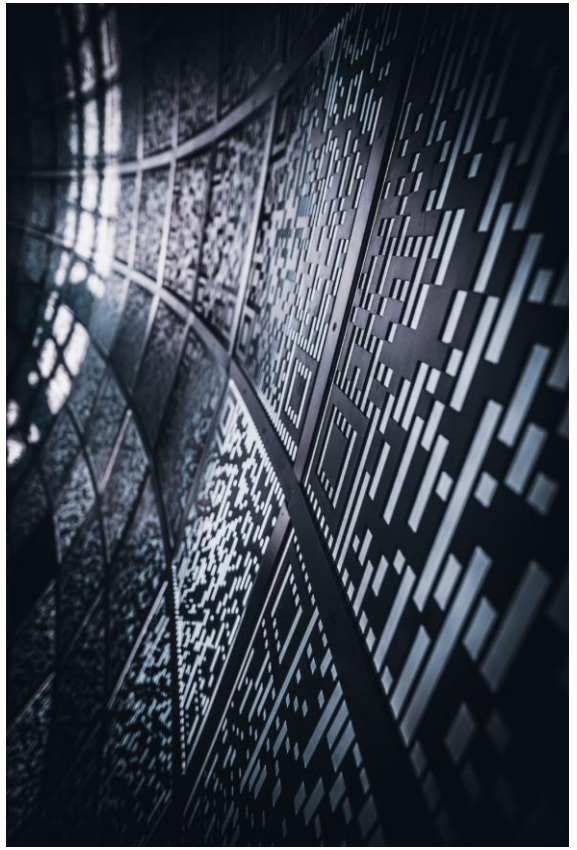
- Online Repository
  - Infrastructure and Capability Assessment
  - Generic Platform Architecture Diagrams
  - Security Control Lists
  - Information Privacy Principles
  - Legislation Summary

https://www.sensitivedataplatforms.org/cops

Better outcomes via collaboration, knowledge sharing, rather than by developing systems in isolation.

Approach: Technical Working Group

- Community Engagement
- Use Case assessments
  - REDCap integration
  - XNAT integration
  - AAF Evaluation
- Conceptual designs for future capabilities



ARDC Australian Research Data Commons

Swansea University Prifysgol Abertawe

MONASH University

QCIF

UNSW SYDNEY

saxinstitute

Curtin University

Approach: Nectar Restricted Region

- Separate ARDC capital investment linked to the deliverables of the ARDC Platform Project

- Strong collaboration with Nectar Core Services to:
  - Build restricted regions in the Nectar Research Cloud
  - Implement strict role-based access control at the Node level
  - Deployed, tested, and rolled into production by QCIF alongside QRIScloud
  - Comprehensive recipes for deploying a Restricted Region in Nectar are available for the other Nodes
  - Improvements rolled into Nectar to uplift security posture

Exemplar Projects

Revitalising Informal Settlements and their Environments (RISE)

Predicting fracture outcomes using Artificial Intelligence (PRAISE)

High Frequency Data Transfer

Machine Learning

Imaging Analysis

Unstructured Data

Data Linkage

Australian Centre of Excellence in Melanoma Imaging & Diagnosis (ACEMID)

ATLAS First Nations Study.

Additional project deliverable

- Develop Minimum set of Characteristics for sensitive data environments.

There are a range of criteria that infrastructure service providers need to minimally meet to successfully deliver research services suitable for handling and analysing sensitive data.

The criteria can be divided into the following categories:

Governance Model and Roles	Policies	Network and Data Security
Service Description	Compliance and Assessment	Data Encryption
Terms and Conditions	Access Controls	Data Segregation
Onboarding and Training	Governance Mechanisms	User Support and Software

Into the future …

- **How do we establish a list of Trusted TREs that are well known to Institutional Ethics Committees and Grant Funding Bodies and considered fit-for-purpose?**

- **How do we best place Australia in a leadership position globally for managing sensitive data for research purposes?**

- **Community agreement for future engagement and collaboration**
  … looking for other interested parties

Discussion

Thank you for joining us today!

Mat Ishac	Monash SeRP	Stephen Bird	KeyPoint
mat.ishac@monash.edu	serp-support@monash.edu	stephen.bird@qcif.edu.au	keypoint@qcif.edu.au