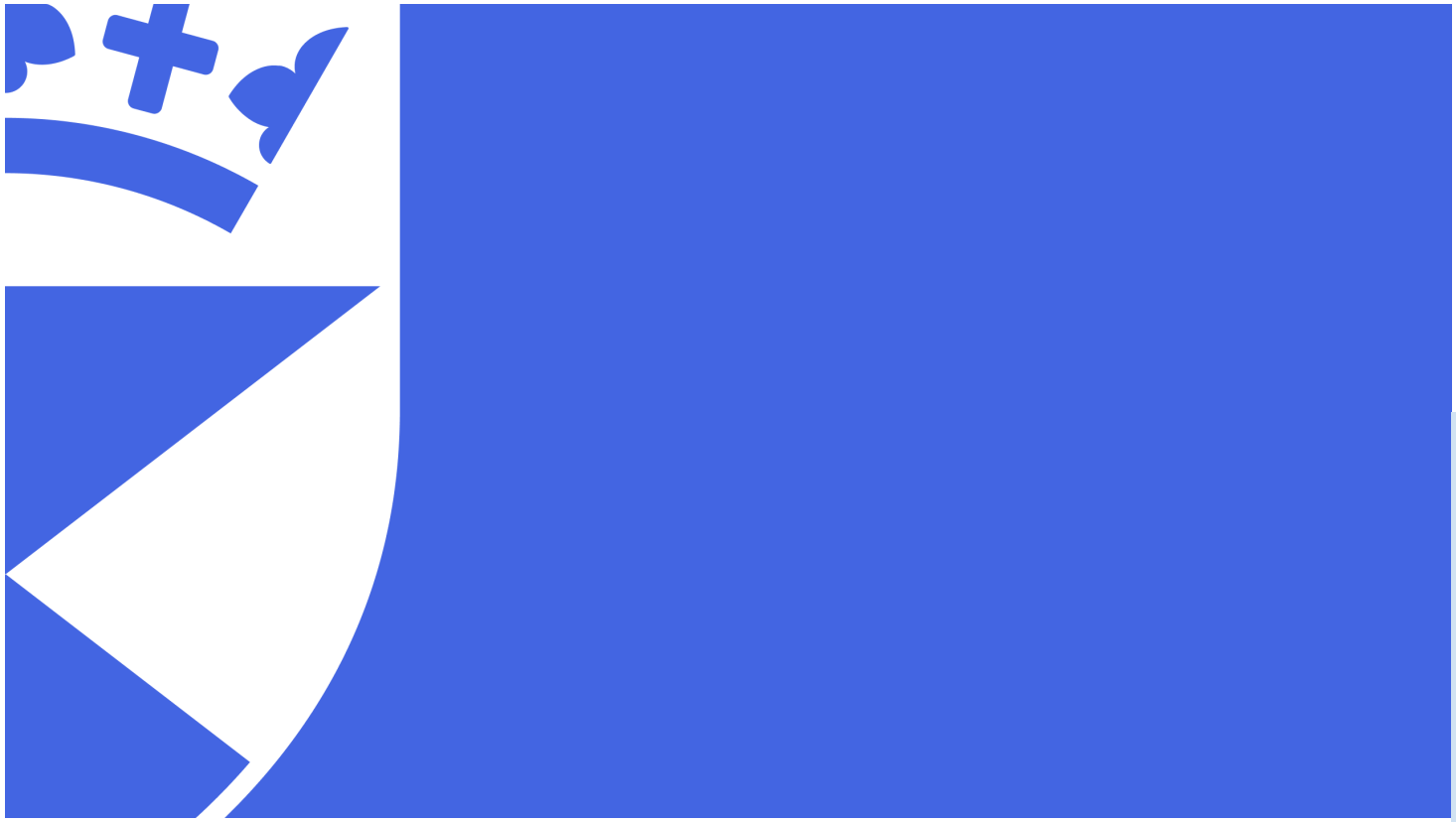


University of Dundee

SATRE - A UK Specification for Trusted Research Environments

Dr Christian Cole – Reader in Health Informatics

Academic Co-Director, Health Informatics Centre

School of Medicine, University of Dundee

The Alan Turing Institute

Ulster University

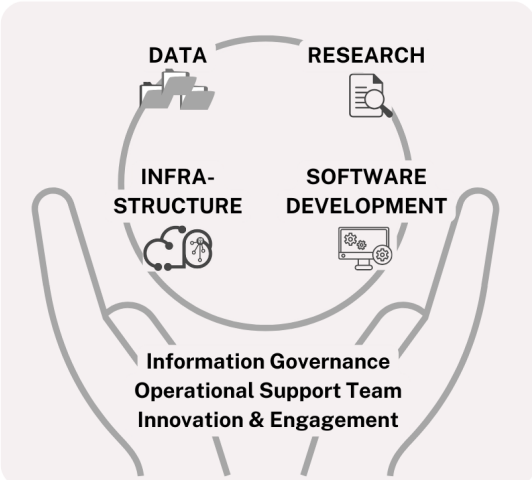
UCL ADVANCED RESEARCH COMPUTING CENTRE UCL

Research Data Scotland

Health Informatics Centre

Health Informatics Centre (HIC)

- Expertise across data linkage and engineering, data science research, software development, infrastructure, information governance and innovation.
- HIC is a data ecosystem, facilitating and drive research, helping building professional networks
- It is the wider expert team working here that make us a Safe Haven.
- HIC are data curators/ processors on behalf of data controllers. We have a balance of responsibilities
  - International
  - UK
  - Scotland
  - Locally
  - Professionally



- 20 Years of Experience
- Circa 40 Staff
- >£170m project support
- >400 research outputs

Health Informatics Centre

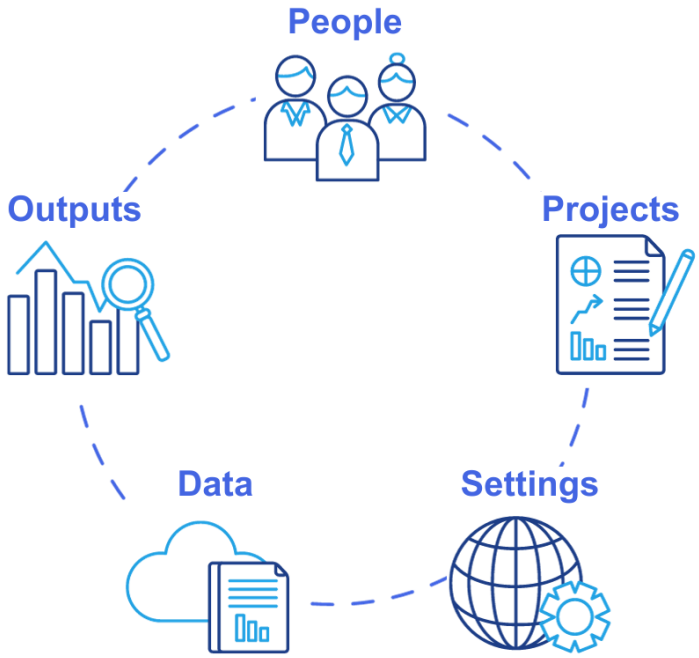
Scottish Safe Haven Network

- Fulfil the needs of the Chief Scientist Office (CSO) Scotland
  - Scottish Safe Haven Charter (2014) accreditation
  - ISO27001 certified
  - >95% population represented
- HIC are 1 of 4 regional Scottish Safe Havens
  - East of Scotland NHS Data
- Run a Trusted Research Environment for >12 years
- Full cost-recovery model

bsi ISO/IEC 27001 Information Security Management CERTIFIED

The Scottish Government

The Five Safes Framework



These best practice processes allow us, as data curators/ TRE providers, to maintain trust and transparency in managing data. We apply proportionate risk mitigation, including the use of our TRE.

1. **Safe People** can access the TRE after training, approvals and our data use declaration are in place.
2. **Safe Projects** are reviewed for public and patient benefit.
3. **Safe Settings** (our TRE) is used to access the data on secure technology systems
4. **Safe Data**, users only use the data that have been pseudonymised to protect privacy
5. **Safe Outputs**, only summary data can be exported out of the TRE, after disclosure control to ensure no potentially sensitive data is released

LANDSCAPE – What's the current context?

TREs are the present and future for sensitive/health data research in the UK and Europe

Department of Health & Social Care

Policy paper

Data saves lives: reshaping health and social care with data

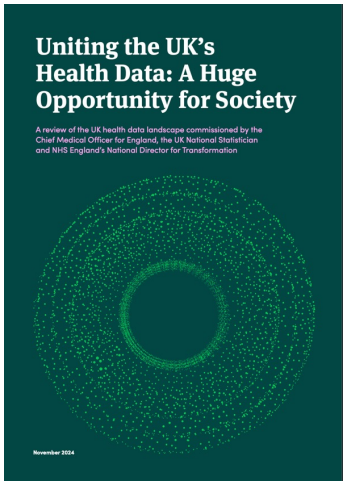
Updated 15 June 2022

DARE UK

Paving the way for a coordinated national infrastructure for sensitive data research

A summary of findings to date from Phase 1 of the UK Research and Innovation DARE UK programme

August 2022



A review commissioned by the Secretary of State for Health and Social Care

Better, Broader, Safer: Using Health Data for Research and Analysis

April 2022

UK Health Data Research Alliance

Building Trusted Research Environments v1.0 dated 8th December 2021

EHDS

HealthData@EU Pilot

eosc | ENTRUST

European Network of Trusted Research Environments

SA TRE

LANDSCAPE - What's the current context?

There are >50 active TRE implementations in the UK. More in development...

Infrastructure choices

Cloud

On-prem

Development models

Community-driven

Commercial

Governance & Accreditation

Regulatory requirements

ISO27001, DEA, DSPT...

Risk appetites

SA TRE

DESIGN WORK - SATRE

Using a **community-driven approach** to build a **reference TRE architecture specification** and **accompanying implementation**

Learn & Explore

Simplify & Specify

Guide & Sustain

Transparency and Openness – Core Principle

Open Code/Resources:

- github.com/sa-tre
- github.com/sa-tre/satre-specification

Open Documentation:

- satre-specification.readthedocs.io

Open Communication:

- https://medium.com/satre

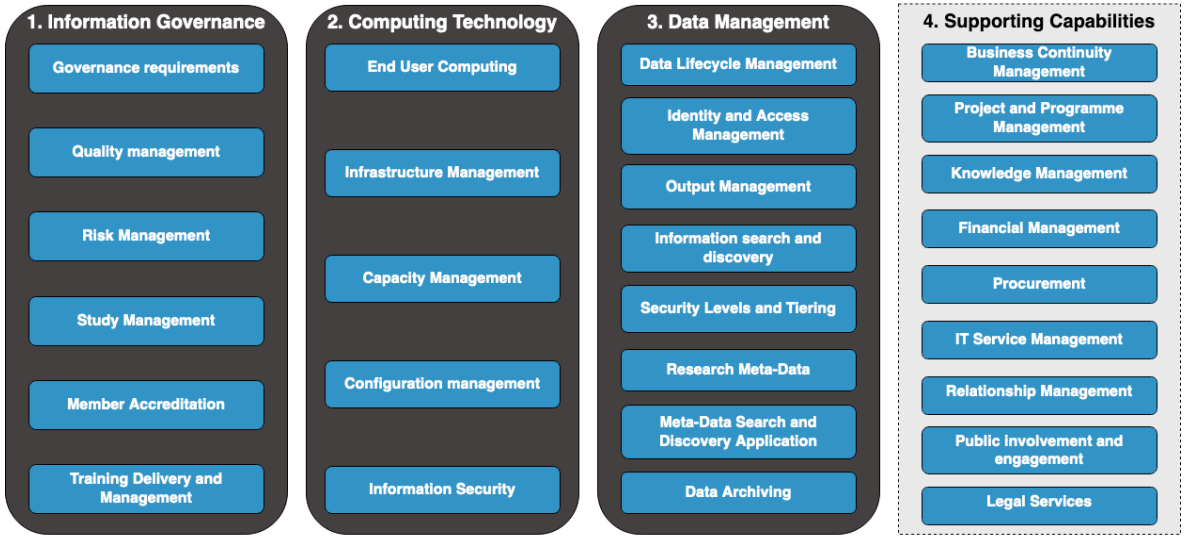
Transparent Information:

- youtube.com/@healthinformaticscentre

What is it?

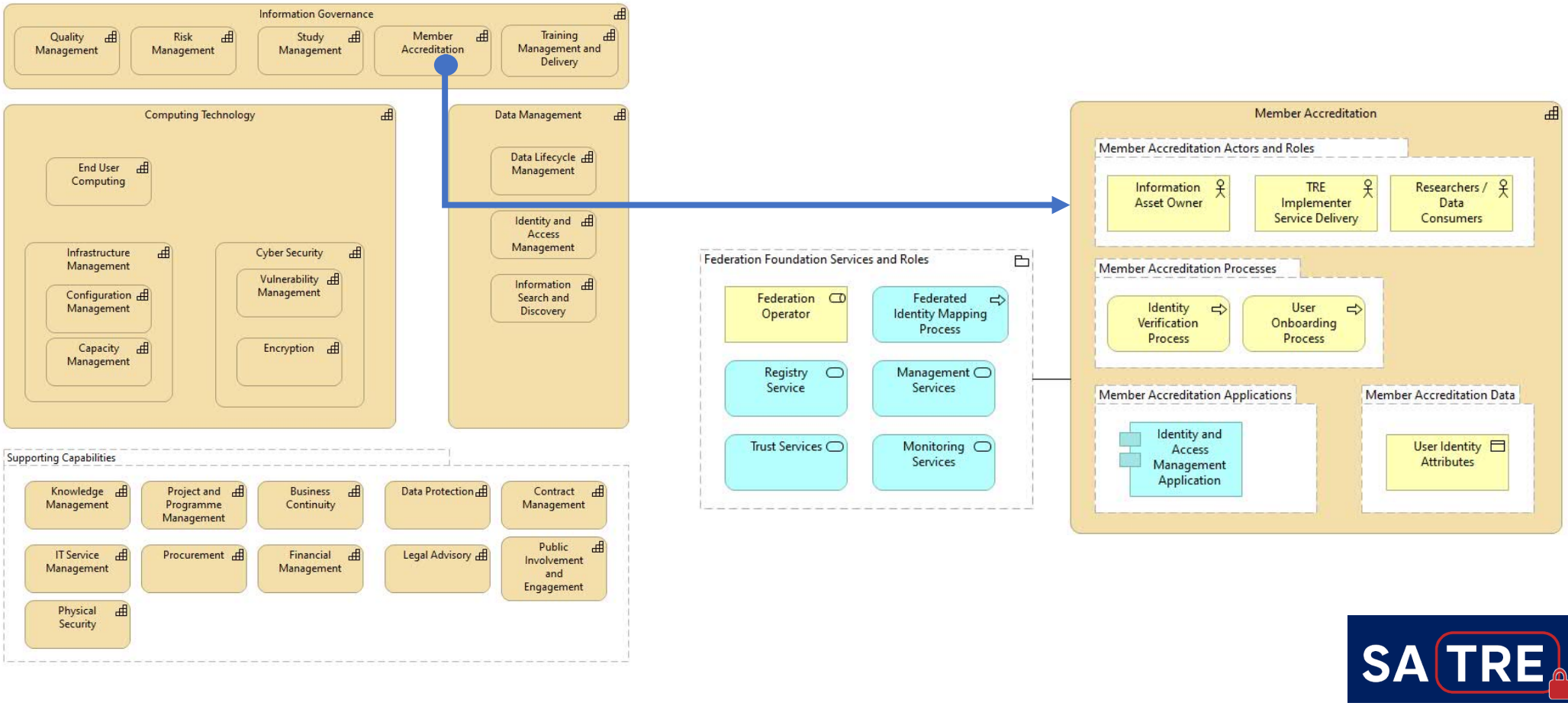
- A guide on how to build and run a TRE
- Four Architectural Principles
  - Usability, Maintaining Public Trust, Observability, Standardisation
- Four Pillars
  - Information Governance
  - Computing Technology
  - Data Management
  - Supporting Capabilities

- 29 Capabilities
  - 160 statements
  - 75 mandatory



Capabilities

Decompositions



A Truly Community-Led Specification

- ~60 organisations engaged
- 14 Collaboration Cafés
- 25 contributors making direct changes to the content

Public Involvement

- Workshops identified transparency as a key requirement
- Reflected in three (mandatory) statements

- Version 1.0 Released Oct 2023

SA TRE

Standard Architecture for Trusted Research Environments (SATRE)

👀 What is SATRE?

The SATRE project provides a Standard Architecture for Trusted Research Environments (TREs). It incorporates knowledge and best practices from multiple institutions and sectors across the UK. This includes all aspects of TRE provision such as information governance procedures, computing technology, data management and other capabilities.

It aims to standardise the capabilities of TREs, making it easier for users, operators, and developers to work with sensitive data, and making the operation of TREs more transparent to data owners and the general public.

This specification should be useful if you are:

- a TRE Operator wanting to evaluate or improve their TRE with the suggested capabilities
- a Developer or Builder of new TREs looking for guidance in their thinking and decision making

We encourage all TREs in the UK to evaluate themselves against the SATRE specification, and to contribute to the project.

Getting started

SA TRE

Evaluation Spreadsheet

	A	B	C	D	E	F	
1	**Section**	**Item**	**Statement**	**Guidance**	**Importance**	**Score**	**Response**
2	Information governance	1.1.1.	You must gather and monitor the information governance requirements needed to fulfil any legal, regulatory and ethical standards.	Requirements will come from a variety of sources including legislation, contractual obligations and ethical standards. Requirements must be monitored to ensure the TRE controls remain appropriate.	Mandatory		
3	Information governance	1.1.2.	You must ensure controls are implemented to ensure the requirements are met.	Control implementation should be systematic and directly aligned to the internal and stakeholder requirements.	Mandatory		
4	Information governance	1.1.3.	You must ensure there are adequate resources to meet information governance requirements.	Ensuring information governance controls are suitable and enforced requires an investment of funding and people appropriate to the size of the TRE.	Mandatory		
5	Information governance	1.2.1.	You must ensure that changes to policies and standard operating procedures can only be made by trusted individuals.	It is important to ensure that policies and SOPs are relevant, up-to-date and carefully controlled to maintain the integrity and security of your TRE organisation.	Mandatory		
6	Information governance	1.2.2.	You must use versioning and a codified change procedure for all policies and standard operating procedures.	This includes recording dates of changes, person responsible for carrying out changes, and summary of changes.	Mandatory		
7	Information governance	1.2.3.	You should measure the performance of information governance within the TRE with regular reporting available to your TRE organisation's management team.	This may include reports and dashboards showing security incidents, quality management deviations and audit findings.	Recommended		
8	Information governance	1.2.4.	You must audit your TRE organisation against relevant requirements and standards.	If you are publicly accredited against a standard, for instance ISO27001, DSPT, CE+ *etc.*, you must have processes in place to ensure you remain compliant.	Mandatory		
9	Information governance	1.2.5.	You must report on and share outcomes of each audit of your TRE organisation with the required bodies.	This may include regulatory bodies or the organisations that manage accreditations you have.	Mandatory		
10	Information governance	1.2.6.	You must ensure that suppliers, contractors and sub-contractors with access to your TRE align with your security requirements.	These should be included as mandatory, non-functional requirements in during procurement and contracting. This will also include contractor staff contracts for example, legal liability and NDAs.	Mandatory		
11	Information governance	1.2.7.	You must monitor compliance of your suppliers with the terms of the contracts.	This will include monitoring changes in the services and infrastructure being delivered and quality management within the contractor's organisation. This may be done through formal audit or by monitoring change and quality documentation provided by the supplier.	Mandatory		
12	Information governance	1.2.8.	You must track and maintain any physical assets used by your TRE.	All physical assets should be maintained and covered by warranty if applicable. At the end of their lifetime, assets should be securely disposed of in such a way that data cannot be recovered from them.	Mandatory (where physical assets are in scope)		
13	Information governance	1.2.9.	You must log, track and resolve any issues resulting from deviations from processes, incidents and audit findings.	This process could, for example, be tracked through an electronic record and workflow system with records retained.	Mandatory		
14	Information governance	1.2.10.	You must use reported issues to inform changes, such as for process improvement and risk management.	All issues should be analysed for their root cause and improvements put in place to prevent further occurrence.	Mandatory		
15	Information governance	1.2.11.	You should collect and maintain quality management data for measuring the effectiveness of a TRE.	Large amounts of data will be produced by elements within the TRE. These data should be analysed with reports and dashboards provided to guide TRE implementer's improvements and provide re-assurance to data consumers and data subjects.	Recommended		
16	Information governance	1.2.12.	You could use a QMS (Quality Management System) to standardise and automate quality management tasks and workflows, and to generate quality data and reports automatically.	A basic QMS could be a set of spreadsheets or documents held in a repository which are manually maintained. More mature applications will provide workflows and generate quality data through manual and automated actions.	Optional		

SA TRE

Self-Assessment

- Whole of Scottish Safe Haven Network: 4 regional and 1 national TRE
  - Federated governance project funded by Research Data Scotland (RDS)

- Publicly available evaluations:
  - HIC
  - Alan Turing Institute
  - Crick Institute

  https://satre.uktre.org

SATRE - Implementations

- Aridhia public blog publicising their SATRE evaluation
  - https://www.aridhia.com/blog/satre-standardised-architecture-for-trusted-research-environments-introduction/
- Canon Medical
  - Client specification requirements

- SATRE being used as baseline for EOSC-ENTRUST Horizon Project
  - 26 partners
  - 14 countries

https://eosc-entrust.eu

EOSC | ENTRUST
European Network of Trusted Research Environments

SATRE Implementations

Scotland

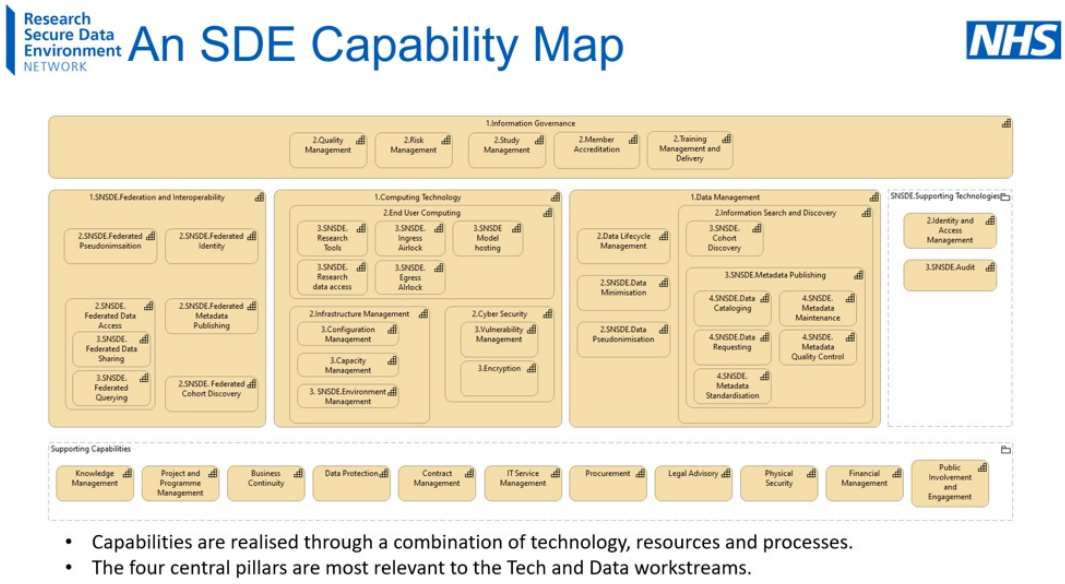
- Review of Scottish Safe Haven Charter (2014) - ScotGov
- Scottish Safe Haven Harmonisation work of the SSHN incl. governance – Research Data Scotland

SDE Accreditation

- Sudlow Review
- DHSC & UK Stats working on Digital Economy Act accreditation for SDEs

England

- Working baseline for SDE network
  - Being led by NHS SCWSU
  - https://github.com/scwcsu/snsde-archi-model



- Capabilities are realised through a combination of technology, resources and processes.
- The four central pillars are most relevant to the Tech and Data workstreams.

Domain Relevance

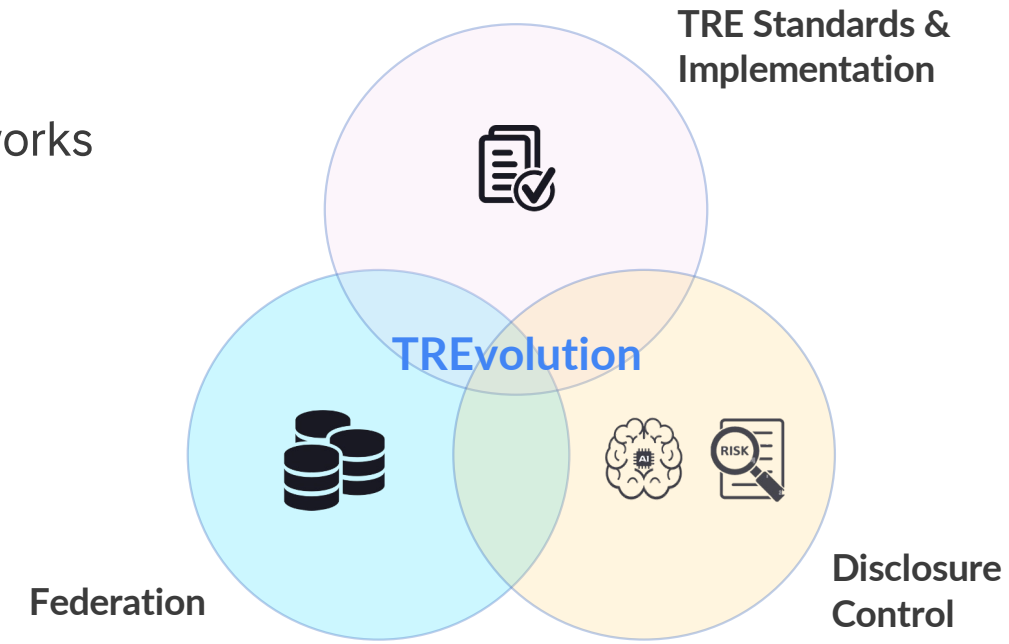
- Extensive experience of real-world use of TREs within highly regulated environments
  - Population census data
  - Health care data
  - Administrative data
- SATRE specification embeds wide-ranging views of TRE stakeholders
  - Fills gaps between implementation and business processes
  - Suits governance, data, industry and academic organisations
  - Reflects public opinion (in UK)
- Open, transparent and adaptable
- Collaborative

SA TRE

DARE UK

Future Plans

- Version 2.0 (in 2025)
  - Respond to community testing
  - Add support for federated TRE networks
  - Add support for AI/ML capability
- Improve evaluation process
  - Development of a capability model
  - Add maturity model
  - Data Tiering
- Training
- Formal accreditation



Formal announcement next week...

Standard Architecture for Trusted Research Environments

SATRE

https://satre.uktre.org satre-contact@dundee.ac.uk

What are we doing?

Maintaining our best-practice guide to building and operating Trusted Research Environments (TREs)

Finding a sustainable model for SATRE:

- Governance
- Formal accreditation
- Extending SATRE

Who benefits?

Public: Better understanding of what's happening with your data

TRE operators & developers: more sharing of knowledge and technology

Users: More consistency amongst TREs

Get involved

UK TRE

https://uktre.org

Safe Data Access Professionals

https://securedatagroup.org

Join a collaboration café

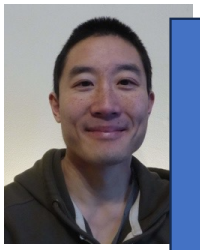
NFCS Pillars

- Communication ✅
  - SATRE IG, TREvolution, HIC
- Technology ✅
  - HIC, TREvolution
- Governance ✅✅
  - SATRE, HIC, DARE IGIG, TREvolution

Acknowledgements

TREEHOOSE/AWS

Dr Christian Cole (PI, AWS TRE)



Dr Simon Li (H AWS TRE)

Prof. Sonya Coleman (SMDH)

Dr Dermott Kerr (SMDH)

HDR UK

Dr Justin Quinn (SMDH)

Public & Stakeholder Engagement

Jilll Beggs Lay Participant

Hari Sood (Turing, SocRSE)

Turing/Azure

James erington Azure

Dr Martin O'Reilly (Turing TRE)

Dr James Robinson (Turing TRE)

Dr Cian O'Donovan (UCL, Azure TRE)

Katie Oldfield (RDS)
Ed Chalstrey (Turing)
Jim Madge (Turing)
Nels Swanepoel (UCL)
Arron Lacey (Turing)
David Sarmiento Perez (Turing)
Tim Machin (UCL)
Matt Craddock (Turing)

UK Research and Innovation

HDRUK Health Data Research UK

ADR UK Data-driven change

University of Dundee

DARE UK

The Alan Turing Institute

Ulster University

UCL ADVANCED RESEARCH COMPUTING CENTRE UCL

Research Data Scotland

Health Informatics Centre

https://satre-specification.readthedocs.io

https://www.dundee.ac.uk/hic

c.cole@dundee.ac.uk