University of Dundee

SATRE - A National Specification for Trusted Research Environments

Dr Simon Li
Dr Christian Cole
Health Informatics Centre, University of Dundee

Funded by
the European Union

eosc | ENTRUST
European Network of Trusted Research Environments

Standard Architecture for Trusted Research Environments

SATRE

Health Informatics Centre

UCL ADVANCED RESEARCH COMPUTING CENTRE
UCL

The Alan Turing Institute

Ulster University

Research Data Scotland

Why did we create SATRE?

1. TREs are the future for sensitive/health data research in the UK

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

Why did we create SATRE?

2. There are currently a large number of TRE implementations in the UK, with many different approaches

Infrastructure choices

Cloud
On-prem

Development models

Community-driven
Commercial

Governance & Accreditation

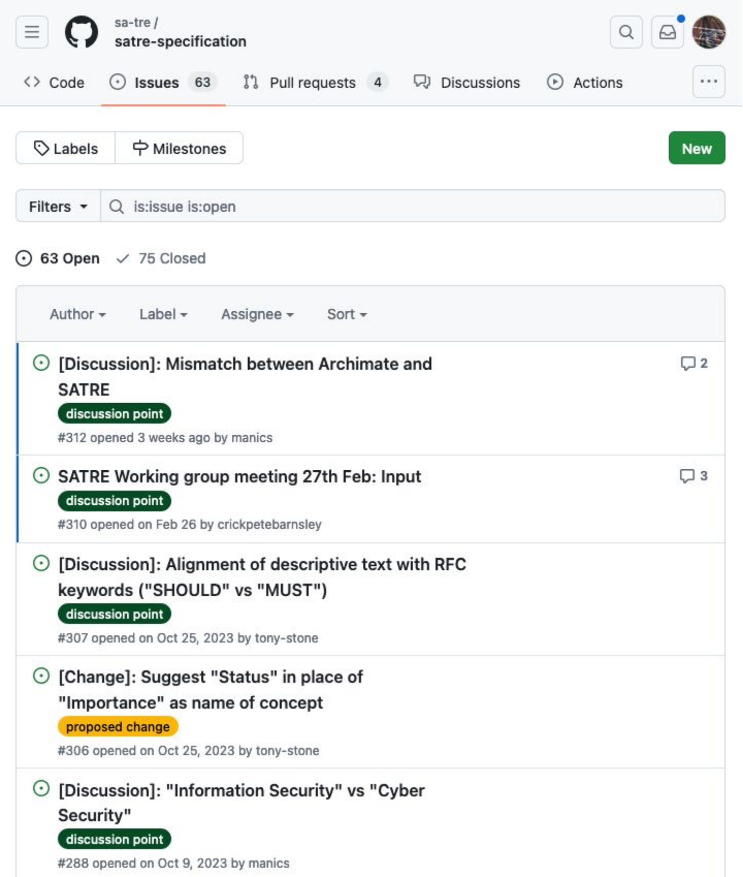
Regulatory requirements
ISO27001, CE+, DSPT...
Risk appetites

Transparency and Openness – Core Principle

Everything was open from the start

All discussions were and continue to be public

https://github.com/sa-tre/satre-specification/issues



63 Open ✓ 75 Closed

[Discussion]: Mismatch between Archimate and SATRE
discussion point
#312 opened 3 weeks ago by manics
2

SATRE Working group meeting 27th Feb: Input
discussion point
#310 opened on Feb 26 by crickpetebarnsley
3

[Discussion]: Alignment of descriptive text with RFC keywords ("SHOULD" vs "MUST")
discussion point
#307 opened on Oct 25, 2023 by tony-stone

[Change]: Suggest "Status" in place of "Importance" as name of concept
proposed change
#306 opened on Oct 25, 2023 by tony-stone

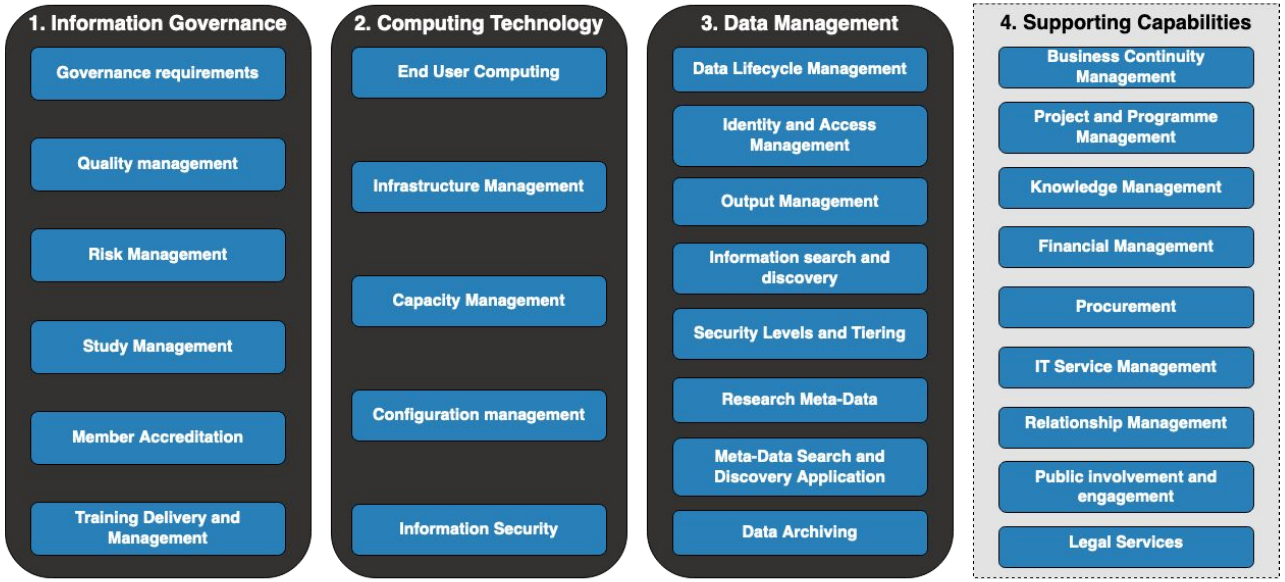
[Discussion]: "Information Security" vs "Cyber Security"
discussion point
#288 opened on Oct 9, 2023 by manics

A UK-wide Community-Led Specification

- 60+ organisations engaged
- Content, direction and delivery shaped by the community
  - E.g. Information Governance
- Feature Survey – 105 responses
- 14 Collaboration Cafés
- 25 contributors making direct (GitHub) changes to the content
- Public involvement workshops:
  - Transparency is a key requirement
  - Reflected in SATRE

What is it?

- A guide on how to build and run a TRE
- Four Pillars
  - Information Governance
  - Computing Technology
  - Data Management
  - Supporting Capabilities
- 29 Capabilities
  - 160 statements
    - 75 mandatory
- Applicable to almost all UK TREs



1. Information Governance

- Governance requirements
- Quality management
- Risk Management
- Study Management
- Member Accreditation
- Training Delivery and Management

2. Computing Technology

- End User Computing
- Infrastructure Management
- Capacity Management
- Configuration management
- Information Security

3. Data Management

- Data Lifecycle Management
- Identity and Access Management
- Output Management
- Information search and discovery
- Security Levels and Tiering
- Research Meta-Data
- Meta-Data Search and Discovery Application
- Data Archiving

4. Supporting Capabilities

- Business Continuity Management
- Project and Programme Management
- Knowledge Management
- Financial Management
- Procurement
- IT Service Management
- Relationship Management
- Public involvement and engagement
- Legal Services

https://satre-specification.readthedocs.io

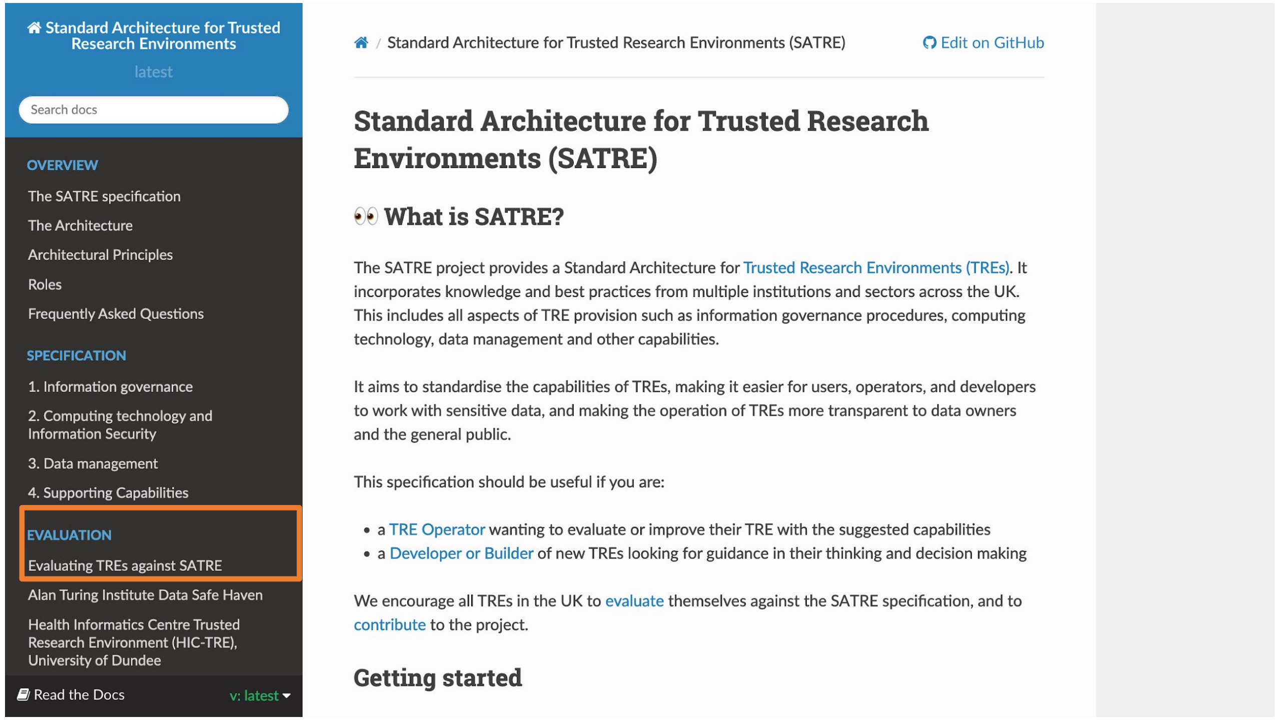
Evaluation: Scoring system

Statements are either

- **Mandatory**
- **Recommended**
- **Optional**

Each statement is scored

- 0 – requirement not met
- 1 – sufficient (could be better)
- 2 – satisfied
- N/A – not applicable


Standard Architecture for Trusted Research Environments
latest
Search docs
OVERVIEW
The SATRE specification
The Architecture
Architectural Principles
Roles
Frequently Asked Questions
SPECIFICATION
1. Information governance
2. Computing technology and Information Security
3. Data management
4. Supporting Capabilities
EVALUATION
Evaluating TREs against SATRE
Alan Turing Institute Data Safe Haven
Health Informatics Centre Trusted Research Environment (HIC-TRE), University of Dundee
Read the Docs
v: latest
/ Standard Architecture for Trusted Research Environments (SATRE)
Edit on GitHub

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:

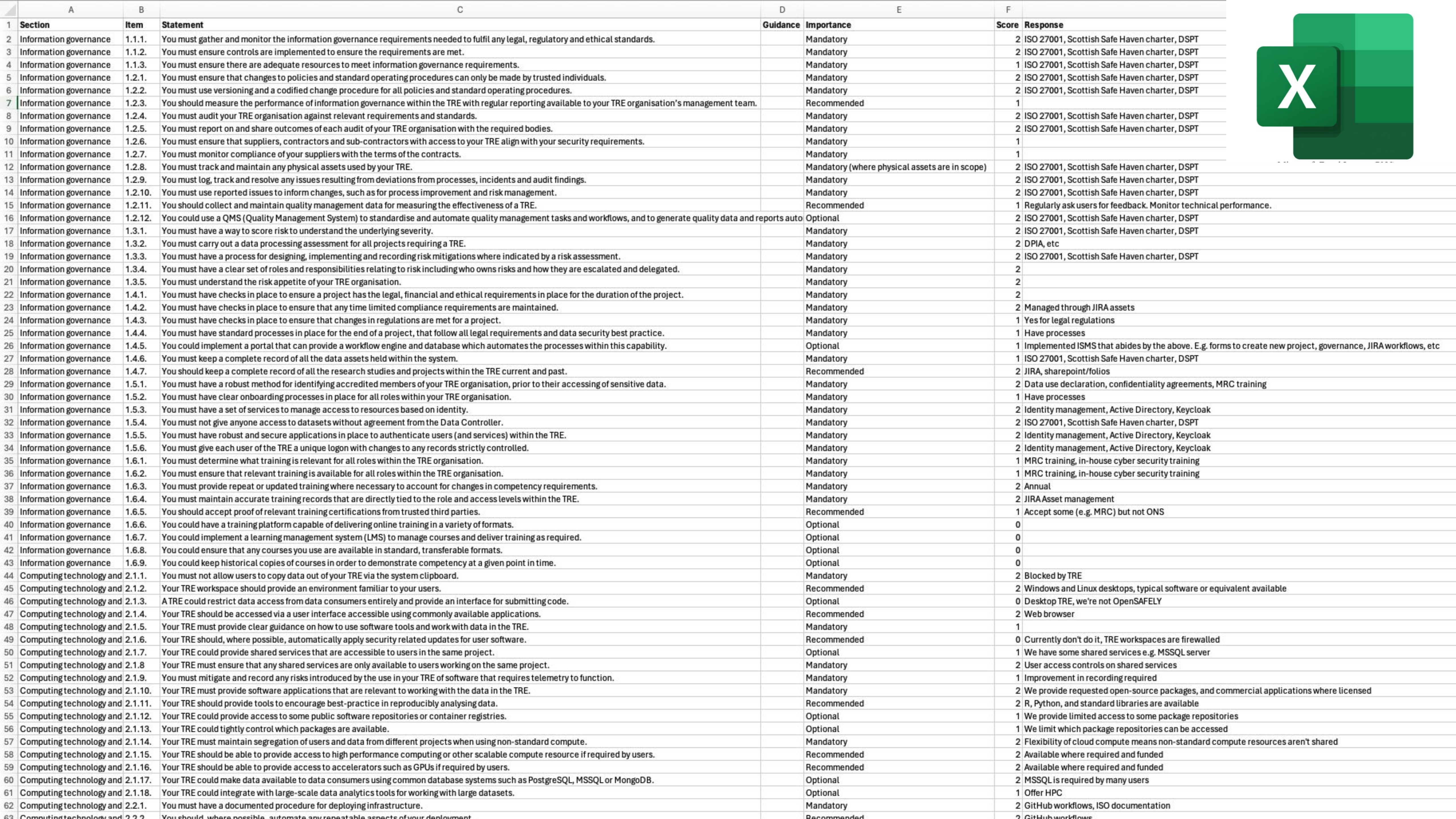
- a TRE Operator wanting to evaluate or improve their TRE with the suggested capabilities
- a Developer or Builder of new TREs looking for guidance in their thinking and decision making

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

Getting started

TREs should score **1+ on mandatory statements**

- 1 or 2: An optional way to identify improvements/gaps



	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.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
3	Information governance	1.1.2.	You must ensure controls are implemented to ensure the requirements are met.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
4	Information governance	1.1.3.	You must ensure there are adequate resources to meet information governance requirements.		Mandatory	1	ISO 27001, Scottish Safe Haven charter, DSPT
5	Information governance	1.2.1.	You must ensure that changes to policies and standard operating procedures can only be made by trusted individuals.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
6	Information governance	1.2.2.	You must use versioning and a codified change procedure for all policies and standard operating procedures.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
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.		Recommended	1	
8	Information governance	1.2.4.	You must audit your TRE organisation against relevant requirements and standards.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
9	Information governance	1.2.5.	You must report on and share outcomes of each audit of your TRE organisation with the required bodies.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
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.		Mandatory	1	
11	Information governance	1.2.7.	You must monitor compliance of your suppliers with the terms of the contracts.		Mandatory	1	
12	Information governance	1.2.8.	You must track and maintain any physical assets used by your TRE.		Mandatory (where physical assets are in scope)	2	ISO 27001, Scottish Safe Haven charter, DSPT
13	Information governance	1.2.9.	You must log, track and resolve any issues resulting from deviations from processes, incidents and audit findings.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
14	Information governance	1.2.10.	You must use reported issues to inform changes, such as for process improvement and risk management.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
15	Information governance	1.2.11.	You should collect and maintain quality management data for measuring the effectiveness of a TRE.		Recommended	1	Regularly ask users for feedback. Monitor technical performance.
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 auto		Optional	2	ISO 27001, Scottish Safe Haven charter, DSPT
17	Information governance	1.3.1.	You must have a way to score risk to understand the underlying severity.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
18	Information governance	1.3.2.	You must carry out a data processing assessment for all projects requiring a TRE.		Mandatory	2	DPIA, etc
19	Information governance	1.3.3.	You must have a process for designing, implementing and recording risk mitigations where indicated by a risk assessment.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
20	Information governance	1.3.4.	You must have a clear set of roles and responsibilities relating to risk including who owns risks and how they are escalated and delegated.		Mandatory	2	
21	Information governance	1.3.5.	You must understand the risk appetite of your TRE organisation.		Mandatory	2	
22	Information governance	1.4.1.	You must have checks in place to ensure a project has the legal, financial and ethical requirements in place for the duration of the project.		Mandatory	2	
23	Information governance	1.4.2.	You must have checks in place to ensure that any time limited compliance requirements are maintained.		Mandatory	2	Managed through JIRA assets
24	Information governance	1.4.3.	You must have checks in place to ensure that changes in regulations are met for a project.		Mandatory	1	Yes for legal regulations
25	Information governance	1.4.4.	You must have standard processes in place for the end of a project, that follow all legal requirements and data security best practice.		Mandatory	1	Have processes
26	Information governance	1.4.5.	You could implement a portal that can provide a workflow engine and database which automates the processes within this capability.		Optional	1	Implemented ISMS that abides by the above. E.g. forms to create new project, governance, JIRA workflows, etc
27	Information governance	1.4.6.	You must keep a complete record of all the data assets held within the system.		Mandatory	1	ISO 27001, Scottish Safe Haven charter, DSPT
28	Information governance	1.4.7.	You should keep a complete record of all the research studies and projects within the TRE current and past.		Recommended	2	JIRA, sharepoint/folios
29	Information governance	1.5.1.	You must have a robust method for identifying accredited members of your TRE organisation, prior to their accessing of sensitive data.		Mandatory	2	Data use declaration, confidentiality agreements, MRC training
30	Information governance	1.5.2.	You must have clear onboarding processes in place for all roles within your TRE organisation.		Mandatory	1	Have processes
31	Information governance	1.5.3.	You must have a set of services to manage access to resources based on identity.		Mandatory	2	Identity management, Active Directory, Keycloak
32	Information governance	1.5.4.	You must not give anyone access to datasets without agreement from the Data Controller.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
33	Information governance	1.5.5.	You must have robust and secure applications in place to authenticate users (and services) within the TRE.		Mandatory	2	Identity management, Active Directory, Keycloak
34	Information governance	1.5.6.	You must give each user of the TRE a unique logon with changes to any records strictly controlled.		Mandatory	2	Identity management, Active Directory, Keycloak
35	Information governance	1.6.1.	You must determine what training is relevant for all roles within the TRE organisation.		Mandatory	1	MRC training, in-house cyber security training
36	Information governance	1.6.2.	You must ensure that relevant training is available for all roles within the TRE organisation.		Mandatory	1	MRC training, in-house cyber security training
37	Information governance	1.6.3.	You must provide repeat or updated training where necessary to account for changes in competency requirements.		Mandatory	2	Annual
38	Information governance	1.6.4.	You must maintain accurate training records that are directly tied to the role and access levels within the TRE.		Mandatory	2	JIRA Asset management
39	Information governance	1.6.5.	You should accept proof of relevant training certifications from trusted third parties.		Recommended	1	Accept some (e.g. MRC) but not ONS
40	Information governance	1.6.6.	You could have a training platform capable of delivering online training in a variety of formats.		Optional	0	
41	Information governance	1.6.7.	You could implement a learning management system (LMS) to manage courses and deliver training as required.		Optional	0	
42	Information governance	1.6.8.	You could ensure that any courses you use are available in standard, transferable formats.		Optional	0	
43	Information governance	1.6.9.	You could keep historical copies of courses in order to demonstrate competency at a given point in time.		Optional	0	
44	Computing technology and	2.1.1.	You must not allow users to copy data out of your TRE via the system clipboard.		Mandatory	2	Blocked by TRE
45	Computing technology and	2.1.2.	Your TRE workspace should provide an environment familiar to your users.		Recommended	2	Windows and Linux desktops, typical software or equivalent available
46	Computing technology and	2.1.3.	A TRE could restrict data access from data consumers entirely and provide an interface for submitting code.		Optional	0	Desktop TRE, we're not OpenSAFELY
47	Computing technology and	2.1.4.	Your TRE should be accessed via a user interface accessible using commonly available applications.		Recommended	2	Web browser
48	Computing technology and	2.1.5.	Your TRE must provide clear guidance on how to use software tools and work with data in the TRE.		Mandatory	1	
49	Computing technology and	2.1.6.	Your TRE should, where possible, automatically apply security related updates for user software.		Recommended	0	Currently don't do it, TRE workspaces are firewalled
50	Computing technology and	2.1.7.	Your TRE could provide shared services that are accessible to users in the same project.		Optional	1	We have some shared services e.g. MSSQL server
51	Computing technology and	2.1.8	Your TRE must ensure that any shared services are only available to users working on the same project.		Mandatory	2	User access controls on shared services
52	Computing technology and	2.1.9.	You must mitigate and record any risks introduced by the use in your TRE of software that requires telemetry to function.		Mandatory	1	Improvement in recording required
53	Computing technology and	2.1.10.	Your TRE must provide software applications that are relevant to working with the data in the TRE.		Mandatory	2	We provide requested open-source packages, and commercial applications where licensed
54	Computing technology and	2.1.11.	Your TRE should provide tools to encourage best-practice in reproducibly analysing data.		Recommended	2	R, Python, and standard libraries are available
55	Computing technology and	2.1.12.	Your TRE could provide access to some public software repositories or container registries.		Optional	1	We provide limited access to some package repositories
56	Computing technology and	2.1.13.	Your TRE could tightly control which packages are available.		Optional	1	We limit which package repositories can be accessed
57	Computing technology and	2.1.14.	Your TRE must maintain segregation of users and data from different projects when using non-standard compute.		Mandatory	2	Flexibility of cloud compute means non-standard compute resources aren't shared
58	Computing technology and	2.1.15.	Your TRE should be able to provide access to high performance computing or other scalable compute resource if required by users.		Recommended	2	Available where required and funded
59	Computing technology and	2.1.16.	Your TRE should be able to provide access to accelerators such as GPUs if required by users.		Recommended	2	Available where required and funded
60	Computing technology and	2.1.17.	Your TRE could make data available to data consumers using common database systems such as PostgreSQL, MSSQL or MongoDB.		Optional	2	MSSQL is required by many users
61	Computing technology and	2.1.18.	Your TRE could integrate with large-scale data analytics tools for working with large datasets.		Optional	1	Offer HPC
62	Computing technology and	2.2.1.	You must have a documented procedure for deploying infrastructure.		Mandatory	2	GitHub workflows, ISO documentation
63	Computing technology and	2.2.2.	You should, where possible, automate any repeatable aspects of your deployment.		Recommended	2	GitHub workflows

Example (HIC-TRE)

Section: Information governance

Item: 1.5.3

Statement: You must have a set of services to manage access to resources based on identity.

Guidance: This will include a security model for role based access with technical controls to ensure the principle of least privilege is enforced.

Importance: Mandatory

HIC-TRE

Score: 2

Response: Identity management, Active Directory, Keycloak

Example (HIC-TRE)

Section: Data management

Item: 3.1.2

Statement: You should keep records of data handling decisions.

Guidance: Decisions that are made as part of the process discussed above should be recorded and made available for inspection by all stakeholders.

Importance: Recommended

HIC-TRE

Score: 1

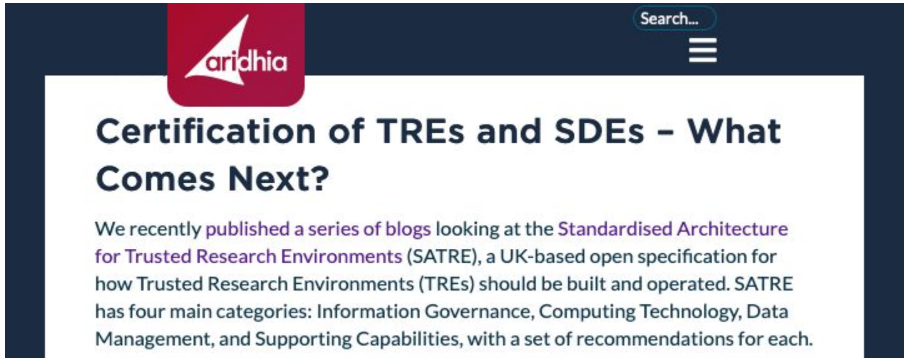
Response: Everything is in project management system. Could make it easier to search old decisions.

How is SATRE being adopted in the UK?

Involvement of the community from the beginning means everyone feels ownership of SATRE

- Open discussions ensure transparency and trust
- Public engagement reassures data controllers

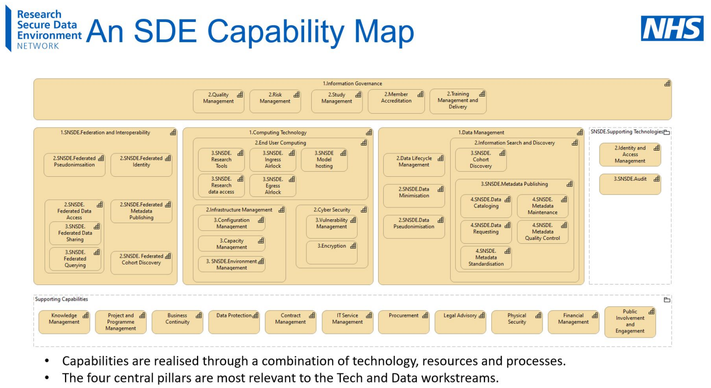
Industry: Several commercial TRE providers are using SATRE



Certification of TREs and SDEs – What Comes Next?

We recently published a series of blogs looking at the Standardised Architecture for Trusted Research Environments (SATRE), a UK-based open specification for how Trusted Research Environments (TREs) should be built and operated. SATRE has four main categories: Information Governance, Computing Technology, Data Management, and Supporting Capabilities, with a set of recommendations for each.

England: SDE network using SATRE as a baseline



An SDE Capability Map

Research Secure Data Environment NETWORK
NHS
1.Information Governance
2.Quality Management
2.Risk Management
2.Study Management
2.Member Accreditation
2.Training Management and Delivery
1.SNSDE.Federation and Interoperability
2.SNSDE.Federated Pseudonimsaition
2.SNSDE.Federated Identity
2.SNSDE. Federated Data Access
3.SNSDE. Federated Data Sharing
3.SNSDE. Federated Querying
2.SNSDE.Federated Metadata Publishing
2.SNSDE. Federated Cohort Discovery
1.Computing Technology
2.End User Computing
3.SNSDE. Research Tools
3.SNSDE. Ingress Airlock
3.SNSDE Model hosting
3.SNSDE. Research data access
3.SNSDE. Egress Alrlock
2.Infrastructure Management
3.Configuration Management
3.Capacity Management
3. SNSDE.Environment Management
2.Cyber Security
3.Vulnerability Management
3.Encryption
1.Data Management
2.Data Lifecycle Management
2.SNSDE.Data Minimisation
2.SNSDE.Data Pseudonimisation
2.Information Search and Discovery
3.SNSDE. Cohort Discovery
3.SNSDE.Metadata Publishing
4.SNSDE.Data Cataloging
4.SNSDE. Metadata Maintenance
4.SNSDE.Data Requesting
4.SNSDE. Metadata Quality Control
4.SNSDE. Metadata Standardisation
SNSDE.Supporting Technologies
2.Identity and Access Management
3.SNSDE.Audit
Supporting Capabilities
Knowledge Management
Project and Programme Management
Business Continuity
Data Protection
Contract Management
IT Service Management
Procurement
Legal Advisory
Physical Security
Financial Management
Public Involvement and Engagement

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

Scotland: All Scottish TREs are evaluating themselves against SATRE

eosc | ENTRUST
European Network of Trusted Research Environments

Supporting ENTRUST

SATRE

- A robust reference point for comparison
  - May or may not be ideal for European environment(s)
  - Relatively quick to apply to identify requirements & capabilities

- Help provide bounds for the blueprint plans
  - What capabilities exist within consortium?

- A good test of SATRE in a new community
  - Identify improvements

Links

SATRE specification

https://satre-specification.readthedocs.io

GitHub organisation

https://github.com/sa-tre

Specification on GitHub

https://github.com/sa-tre/satre-specification eosc

ENTRUST

European Network of Trusted Research Environments

www.eosc-entrust.eu

@eosc_entrust

/company/eosc-entrust

Funded by the European Union

UKRI Innovate UK

eosc | ENTRUST

European Network of Trusted Research Environments