**The Aridhia DRE was originally scored against the SATRE specification in March 2024, in March 2025 the DRE was rescored following the introduction of new features in the previous 12 months. This paper has been updated to reflect the new score.**

Standardised Architecture for Trusted Research Environments (SATRE) is a DARE UK driver project to support the development of a secure reference architecture for Trusted Research Environments (TRE), allowing research teams to benchmark their own TRE against an open specification.

SATRE covers more than the technical implementation of a TRE: it also covers the supporting services required to successfully maintain a secure, legally compliant TRE.

These requirements are broken into four sections, each of which contain a mixture of mandatory and recommended TRE features:

1. Information Governance
2. Computing Technology and Information Security
3. Data Management
4. Supporting Capabilities

**SATRE and the Aridhia DRE**

The Aridhia DRE is an Enterprise Trusted Research Environment, fully managed with deployments across the globe, used by hospitals, research consortia and pharmaceutical companies, and we welcome the emergence and adoption of open specifications for TRE development, as it allows data owners and TRE providers to benchmark their platforms, identify gaps, and therefore drive up overall standards in TRE provision.

This paper scores the Aridhia DRE against the four sections of the SATRE specification, and summarises some of the features that we believe contribute toward that score. A full breakdown of the DRE's score against the SATRE specification is available in the appendix.

**Information Governance**

This section recommends some technical controls, but is primarily concerned with the policies and procedures required to ensure good information governance. This covers a range of activities from ensuring compliance with all legal and regulatory requirements, having clearly defined policies and operating procedures, auditing your TRE against existing standards (e.g. ISO27001), having a robust risk management process in place, and providing TRE users with training material appropriate to their role.

**Overall Score 77/80**

We scored the Aridhia DRE at **77 from a possible 80**, because:

- The Aridhia DRE is certified against a number of recognised international standards (ISO27001, ISO27701 and HITRUST)
- To maintain these certifications the Aridhia DRE is audited annually, and the results made available via our website.
- We provide our customers with comprehensive training materials for all aspects of the DRE, and our project managers can organise bespoke training as required.
- Aridhia has mature and robust risk management procedures in place.

- All data access is controlled by data owners, through a fully configurable data access request process.

### Computing Technology and Information Security

This section contains the main SATRE technical specifications for TRE software and infrastructure. For software this covers ease of access and use, the tools and computing power that should be available to users, and programmatic security measures that should be in place to stop misuse of data. For infrastructure it covers deployment, configuration and maintenance.

This section also includes the requirements for TRE resilience, including agreed service levels, data back-up requirements, infrastructure redundancy, and the need to identify and resolve security vulnerabilities.

**Overall Score 119/122**

The Computing Technology and Information Security section of SATRE is covers both the software and infrastructure requirements for a trusted research environment.

We scored the Aridhia DRE at **119 from a possible 122**, because:

- Aridhia DRE Workspaces provide a secure compute environment with inbound and outbound **airlock review and approval processes**.
- **Data cannot be copied** out of a workspace to a local desktop, data can only leave the workspace via an approved and audited airlock request.
- The workspaces come with a Postgres database, over twenty bioinformatics analysis modules, R-Studio and Jupyter Notebook built in – **without the need to use a virtual machine**.
- Virtual machines are updated with security updates routinely as is the supporting TRE infrastructure.

### Data Management

This section covers a wide range of requirements related to data management from high level product requirements (e.g. users should be provided with a searchable metadata catalogue), to granular user management policies (e.g. multi-user accounts should not be issued). Between these poles it contains a number of recommendations related to data access management from both a policy and technical implementation perspective, requirements for secure and legally compliant data ingress and egress from the TRE, and further requirements for user identification, authentication and management.

**Overall Score 54/62**

The Data Management section of SATRE is concerned with the management of data and metadata, data discoverability, supporting different data types, data access controls, secure ingress and egress of data, and user management and authentication.

We scored the Aridhia DRE at **54 from a possible 62**, because it provides a wide range of features in this area:

- FAIR Data Services is the DRE's native metadata catalogue, which supports a number of existing metadata standards (e.g. OMOP) and allows users to provide their own custom catalogue templates.
- All Data Access Requests in the DRE are managed in a **fully audited and configurable DAR process**.
- Data egress and ingress can be managed through our secure Airlock feature.
- All users log-in with Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC) ensures that **users only have the permission they need**.

**Supporting Capabilities**

This section collects all other supporting services required to successfully maintain a TRE not covered in the previous three sections. These include: project management, business continuity planning, ongoing operational support for software and infrastructure, and access to legal advice regarding data protection and any contracts related to TRE provision. As with the sections above this is only a brief precis of the full specification, but it serves to illustrate the breadth of skills and resources required to successfully build and maintain a secure and legally compliant TRE, something previously explored in our Build vs Buy blog.

**Overall Score 30/30**

We scored the Aridhia DRE at **30 from a possible 30**, because:

- Each Aridhia customer has their own dedicated project manager.
- All Aridhia DRE users have the support of a **full-time service desk team.**
- The Aridhia DRE is backed by a comprehensive business continuity plan which is **tested multiple times per year**.
- All customers can be provided with a full breakdown of the costs for running their projects in the Aridhia DRE.

## Appendix

**(Note on scoring - where a field has been marked as NA, it is not counted as part of the total possible score for that section.)**

**Information Governance in the Aridhia DRE:**

**Overall Score 78/80**

The Information Governance Section of SATRE is covers a wide range of organisational capabilities needed for the successful operation and maintenance of a trusted research environment, from compliance with recognised international standards, to the provision of comprehensive training material for all users.

**SATRE 1.1**

Score 6/6

The Aridhia DRE is certified under a number of widely recognised standards, including ISO27001, ISO27701 and HITRUST. Our dedicated Information Security Team continually monitor our performance against these standards to ensure ongoing compliance.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 1.1.1. | You must gather and monitor the information governance requirements needed to fulfil any legal, regulatory and ethical standards. | Mandatory | 2 |
| 1.1.2. | You must ensure controls are implemented to ensure the requirements are met. | Mandatory | 2 |
| 1.1.3. | You must ensure there are adequate resources to meet information governance requirements. | Mandatory | 2 |

**SATRE 1.2**

21/22

As detailed in section 1.1, the Aridhia DRE is certified against a number of recognised standards. The TRE is audited each year to confirm its compliance with these standards and the results are published to our website. Our Information Security team regularly reviews the security and financial status of all our suppliers.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 1.2.1. | You must ensure that changes to policies and standard operating procedures can only be made by trusted individuals. | Mandatory | 2 |

| | | | |
|---|---|---|---|
| 1.2.2. | You must use versioning and a codified change procedure for all policies and standard operating procedures. | Mandatory | 2 |
| 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 | 2 |
| 1.2.4. | You must audit your TRE organisation against relevant requirements and standards. | Mandatory | 2 |
| 1.2.5. | You must report on and share outcomes of each audit of your TRE organisation with the required bodies. | Mandatory | 2 |
| 1.2.6. | You must ensure that suppliers, contractors and sub-contractors with access to your TRE align with your security requirements. | Mandatory | 2 |
| 1.2.7. | You must monitor compliance of your suppliers with the terms of the contracts. | Mandatory | 2 |
| 1.2.8. | You must track and maintain any physical assets used by your TRE. | Mandatory (where physical assets are in scope) | NA |
| 1.2.9. | You must log, track and resolve any issues resulting from deviations from processes, incidents and audit findings. | Mandatory | 2 |
| 1.2.10. | You must use reported issues to inform changes, such as for process improvement and risk management. | Mandatory | 2 |
| 1.2.11. | You should collect and maintain quality management data for measuring the effectiveness of a TRE. | Recommended | 2 |
| 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. | Optional | 1 |

**SATRE 1.3**

Score 10/10

Aridhia has a mature risk management process in place. A risk register is kept and reviewed at regular intervals, all risks have an assigned owner and are assessed for probability and impact. The Aridhia DRE has a DPIA which is reviewed annually, and we can provide assistance to customers with data processing issues where required.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 1.3.1. | You must have a way to score risk to understand the underlying severity. | Mandatory | 2 |
| 1.3.2. | You must carry out a data processing assessment for all projects requiring a TRE. | Mandatory | 2 |

| | | | |
|---|---|---|---|
| 1.3.3. | You must have a process for designing, implementing and recording risk mitigations where indicated by a risk assessment. | Mandatory | 2 |
| 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 |
| 1.3.5. | You must understand the risk appetite of your TRE organisation. | Mandatory | 2 |

**SATRE 1.4**

Score 12/12

Aridhia provides support to the users of its trusted research environment across the whole lifecycle of a project, from ensuring that data is managed in an ethical and legally compliant way, to managing the removal or deletion of data at the end of a project.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 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 |
| 1.4.2. | You must have checks in place to ensure that any time limited compliance requirements are maintained. | Mandatory | 2 |
| 1.4.3. | You must have checks in place to ensure that changes in regulations are met for a project. | Mandatory | 2 |
| 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 | 2 |
| 1.4.5. | You could implement a portal that can provide a workflow engine and database which automates the processes within this capability. | Optional | 2 |
| 1.4.6. | You must keep a complete record of all the data assets held within the system. | Mandatory | 2 |
| 1.4.7. | You should keep a complete record of all the research studies and projects within the TRE current and past. | Recommended | NA |

**SATRE 1.5**

Score 12/12

All Aridhia staff are identified and accredited. The Aridhia DRE has a number of technical controls in place to ensure that all users are authenticated and identifiable, and each user has a unique logon. Access to all datasets is determined by the Data Owner.

| Item | Statement | Importance | Score |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 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 |
| 1.5.2. | You must have clear onboarding processes in place for all roles within your TRE organisation. | Mandatory | 2 |
| 1.5.3. | You must have a set of services to manage access to resources based on identity. | Mandatory | 2 |
| 1.5.4. | You must not give anyone access to datasets without agreement from the Data Controller. | Mandatory | 2 |
| 1.5.5. | You must have robust and secure applications in place to authenticate users (and services) within the TRE. | Mandatory | 2 |
| 1.5.6. | You must give each user of the TRE a unique logon with changes to any records strictly controlled. | Mandatory | 2 |

**SATRE 1.6**

Score 17/18

All users of the Aridhia DRE have access to our Knowledge Base and online learning platform. These are updated regularly and provide users with a comprehensive overview of the DRE and its capabilities. In addition, every customer has a dedicated project manager who can arrange bespoke training as required.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 1.6.1. | You must determine what training is relevant for all roles within the TRE organisation. | Mandatory | 2 |
| 1.6.2. | You must ensure that relevant training is available for all roles within the TRE organisation. | Mandatory | 2 |
| 1.6.3. | You must provide repeat or updated training where necessary to account for changes in competency requirements. | Mandatory | 2 |
| 1.6.4. | You must maintain accurate training records that are directly tied to the role and access levels within the TRE. | Mandatory | 2 |
| 1.6.5. | You should accept proof of relevant training certifications from trusted third parties. | Recommended | 2 |
| 1.6.6. | You could have a training platform capable of delivering online training in a variety of formats. | Optional | 2 |
| 1.6.7. | You could implement a learning management system (LMS) to manage courses and deliver training as required. | Optional | 2 |
| 1.6.8. | You could ensure that any courses you use are available in standard, transferable formats. | Optional | 1 |
| 1.6.9. | You could keep historical copies of courses in order to demonstrate competency at a given point in time. | Optional | 2 |

**Computing Technology and Information Security in the Aridhia DRE:**

**Overall Score 119/122**

The Computing Technology and Information Security section of SATRE covers both the software and infrastructure requirements for a trusted research environment.

**SATRE 2.1**

Score 34/36

Aridhia DRE Workspaces provide users with secure research spaces that are segregated by project. Where possible, security updates are applied automatically, and where this is not possible they are applied as part of our regular release process. Workspace users have access to Windows and Linux VMs, and a variety of industry-standard tooling including RStudio and Jupyter Notebook. Access to Gitea and a user managed Azure Container Registry (ACR) provide users with version control and software storage capabilities.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 2.1.1. | You must not allow users to copy data out of your TRE via the system clipboard. | Mandatory | 1 |
| 2.1.2. | Your TRE workspace should provide an environment familiar to your users. | Recommended | 2 |
| 2.1.3. | A TRE could restrict data access from data consumers entirely and provide an interface for submitting code. | Optional | 2 |
| 2.1.4. | Your TRE should be accessed via a user interface accessible using commonly available applications. | Recommended | 2 |
| 2.1.5. | Your TRE must provide clear guidance on how to use software tools and work with data in the TRE. | Mandatory | 2 |
| 2.1.6. | Your TRE should, where possible, automatically apply security related updates for user software. | Recommended | 2 |
| 2.1.7. | Your TRE could provide shared services that are accessible to users in the same project. | Optional | 2 |
| 2.1.8 | Your TRE must ensure that any shared services are only available to users working on the same project. | Mandatory | 2 |
| 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 | 2 |
| 2.1.10. | Your TRE must provide software applications that are relevant to working with the data in the TRE. | Mandatory | 2 |

| | | | |
|---|---|---|---|
| 2.1.11. | Your TRE should provide tools to encourage best-practice in reproducibly analysing data. | Recommended | 2 |
| 2.1.12. | Your TRE could provide access to some public software repositories or container registries. | Optional | 2 |
| 2.1.13. | Your TRE could tightly control which packages are available. | Optional | 2 |
| 2.1.14. | Your TRE must maintain segregation of users and data from different projects when using non-standard compute. | Mandatory | 2 |
| 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 |
| 2.1.16. | Your TRE should be able to provide access to accelerators such as GPUs if required by users. | Recommended | 2 |
| 2.1.17. | Your TRE could make data available to data consumers using common database systems such as PostgreSQL, MSSQL or MongoDB. | Optional | 2 |
| 2.1.18. | Your TRE could integrate with large-scale data analytics tools for working with large datasets. | Optional | 1 |

**SATRE 2.2**

Score 32/32

The Aridhia DRE is deployed as a managed service on Azure Cloud. All software changes are thoroughly tested by our QC team in our dedicated test environment before deployment to production. Our service description provides users with an availability target for the DRE. The DRE infrastructure is regularly monitored to identify, document, and resolve misconfigurations and vulnerabilities.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 2.2.1. | You must have a documented procedure for deploying infrastructure. | Mandatory | 2 |
| 2.2.2. | You should, where possible, automate any repeatable aspects of your deployment. | Recommended | 2 |
| 2.2.3. | You must have a documented procedure for making changes to deployed infrastructure. | Mandatory | 2 |
| 2.2.4. | You must test changes before they are used in production. | Mandatory | 2 |
| 2.2.5. | You should have a development environment that mirrors your production environment which you use to test infrastructure changes before committing them to production. | Recommended | 2 |

| | | | |
|---|---|---|---|
| 2.2.6. | You must have a documented procedure for removing infrastructure when it is no longer needed. | Mandatory | 2 |
| 2.2.7. | You should understand the availability and uptime guarantees of any providers that you rely on. | Recommended | 2 |
| 2.2.8. | You should develop an availability target or statement and share this with your users. | Recommended | 2 |
| 2.2.9. | Your TRE must control and manage all of its network infrastructure in order to protect information in systems and applications. | Mandatory | 2 |
| 2.2.10. | Your TRE must not allow connectivity between users in different projects, or with access to different datasets. | Mandatory | 2 |
| 2.2.11. | Your TRE must block outbound connections to the internet by default. | Mandatory | 2 |
| 2.2.12. | You should be able to monitor the network configuration of your TRE to check for misconfigurations and vulnerabilities. | Recommended | 2 |
| 2.2.13. | You should regularly monitor the network configuration of your TRE to check for misconfigurations and vulnerabilities. | Recommended | 2 |
| 2.2.14. | Your TRE must record usage data. | Mandatory | 2 |
| 2.2.15. | Your TRE should record which datasets are accessed, when and by who. | Recommended | 2 |
| 2.2.16. | Your TRE should record computational resource usage at the user or aggregate level. | Recommended | 2 |

**SATRE 2.3**

Score 8/8

Our pricing is fully transparent, with customers aware of the cost of individual workspaces and their associated VMs. Usage cost is monitored on a monthly basis and Azure alerts are in place for forecasted budget breaches.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 2.3.1. | You must ensure that all projects understand what resources are available and what the associated costs will be before the project starts. | Mandatory | 2 |
| 2.3.2. | You should ensure that the anticipated needs of projects can be satisfied using available resources. | Recommended | 2 |
| 2.3.3. | You must have a procedure for allocating available resources among projects. | Mandatory | 2 |
| 2.3.4. | You must ensure that the anticipated resource requirements will not result in overspending by the TRE. | Mandatory | 2 |

**SATRE 2.4**

The Aridhia DRE is deployed using DevOps pipelines with associated procedures which are managed and maintained by Aridhia. Our pipelines then update the configuration each week with a new

release which contains new features and bug fixes, running a combination of automated and manual smoke tests to verify the release. We use a cloud configuration tool to detect anomalies in configuration and set-up.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 2.4.1. | You must have a documented procedure for configuring infrastructure. | Mandatory | 2 |
| 2.4.2. | You should use configuration management tools to automate application of your configuration wherever possible. | Recommended | 2 |
| 2.4.3. | You should be able to verify whether the configuration is valid. | Recommended | 2 |
| 2.4.4. | You should regularly verify your TRE configuration. | Recommended | 2 |
| 2.4.5. | You must be able to replace a non-compliant TRE with a compliant system. | Mandatory | 2 |

**SATRE 2.5**

Score 36/36

The Aridhia DRE is secure and resilient. The DRE is subject to two penetration tests carried out by external contractors annually, with further tests arranged for major feature releases, the results of which are shared with our customers. Aridhia runs quarterly incident response exercises to ensure our incident response procedures are fit for purpose. All DRE hubs have rolling 14-day backups in place to ensure recovery in the event of a major incident. These and other operational processes are detailed in our Knowledge Base. Data is encrypted at rest and in transit.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 2.5.1. | You should keep backups of data and research environments, provided that this is permitted by law. | Recommended | 2 |
| 2.5.2. | You should build redundancy into infrastructure and storage. | Recommended | 2 |
| 2.5.3. | You should keep backups of infrastructure, applications and configurations. | Recommended | 2 |
| 2.5.4. | You must have procedures in place for rapid incident response. | Mandatory | 2 |
| 2.5.5. | You should test your incident response through simulation. | Recommended | 2 |
| 2.5.6. | You should have an application in place to scan for vulnerabilities across infrastructure. | Recommended | 2 |
| 2.5.7. | You must have a process in place for applying security updates to all software that forms part of the TRE infrastructure. | Mandatory | 2 |
| 2.5.8. | Infrastructure should be automatically patched for vulnerabilities. | Recommended | 2 |
| 2.5.9. | You should carry out penetration tests on your TRE. | Recommended | 2 |

| | | | |
|---|---|---|---|
| 2.5.10. | You should update the security controls of your TRE based on the results of security tests. | Recommended | 2 |
| 2.5.11. | You should publish details of your security testing strategy and, where possible, the results of each test. | Recommended | 2 |
| 2.5.12. | Your TRE must encrypt project and user data at rest. | Mandatory | 2 |
| 2.5.13. | Your TRE must encrypt data when in transit between the TRE and external networks or computers. | Mandatory | 2 |
| 2.5.14. | Your TRE should encrypt data when in transit inside the TRE. | Recommended | 2 |
| 2.5.15. | You should use encryption algorithms and software that are widely accepted as secure. | Recommended | 2 |
| 2.5.16. | Your TRE should use secure key management. | Recommended | 2 |
| 2.5.17. | Your TRE could offer physical protection measures against data leakage or theft via physical means. | Optional | 2 |
| 2.5.18. | Your TRE may need to comply with specific regulatory requirements due to the types of data it is hosting. | Mandatory | 2 |

**Data Management in the Aridhia DRE:**

**Overall Score 54/62**

The Data Management section of SATRE is concerned with the management of data and metadata, data discoverability, supporting different data types, data access controls, secure ingress and egress of data, and user management and authentication.

**SATRE 3.1**

Score: 23/26The Aridhia DRE provides users with a variety of technical controls to ensure data is handled in a secure and compliant way, including Role-Based Access Control (RBAC) for all users, a comprehensive audit log, and a secure airlock for data ingress and egress. FAIR external data sources and data federation integrations allow data owners to minimise the amount of data held directly in the TRE.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 3.1.1. | You must have processes in place to assess the legal and regulatory implications of handling the data through its full lifecycle. | Mandatory | 2 |
| 3.1.2. | You should keep records of data handling decisions. | Recommended | 2 |
| 3.1.3. | Information asset owners must classify data sets according to a common process and data classification methodology. | Mandatory | 2 |
| 3.1.4. | You must have a data ingress process which enforces information governance rules/processes. | Mandatory | 1 |
| 3.1.5. | You must have a data egress process which enforces information governance rules/processes. | Mandatory | 2 |
| 3.1.6. | Egress must be limited to the information asset owners or their delegates. | Mandatory | 2 |

| | | | |
|---|---|---|---|
| 3.1.7. | Your data egress process could sometimes require project-independent approval. | Optional | 1 |
| 3.1.8. | You must keep a record of what data your TRE holds. | Mandatory | 2 |
| 3.1.9. | You must have a policy on data deletion. | Mandatory | 2 |
| 3.1.10. | You should have a method of providing proof of deletion/removal of files. | Recommended | 2 |
| 3.1.11. | You should log how input data is modified. | Recommended | 1 |
| 3.1.12. | You must, to a reasonable extent, prevent unauthorised data ingress or egress. | Mandatory | 2 |
| 3.1.13. | Data held within the TRE should be the minimum required for analysis or research. | Recommended | 2 |

**SATRE 3.2**

Score: 12/12

The Aridhia DRE allows customers to set the level of information users must provide to register an account, and all users log-in using multi-factor authentication (MFA). All data access is managed through a fully configurable Data Access Request (DAR) process, which allows data owners to control who has access to their datasets.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 3.2.1. | You must not create user accounts for use by more than one person. | Mandatory | 2 |
| 3.2.2. | You must be reasonably convinced of the identity of each person being granted an account. | Mandatory | 2 |
| 3.2.3. | You must restrict a user's access to only data required in their work. | Mandatory | 2 |
| 3.2.4. | You must ensure that multi-factor authentication is enabled for all users. | Mandatory | 2 |
| 3.2.5. | You could use federated authentication or single sign-on (SSO) for user login. | Optional | 2 |
| 3.2.6. | You could restrict access to particular networks or physical locations. | Optional | 2 |

**SATRE 3.3**

Score: 5/8

This section primarily covers policy questions which are outside of our responsibility as a platform provider. However, our data usage agreements framework, configurable DAR process and data airlock feature provide data owners with a variety of tools for managing data access and project outputs.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 3.3.1. | You should have a system to help classify outputs. | Recommended | 1 |
| 3.3.2. | You should establish the intended outputs of each project from the outset. | Recommended | 2 |
| 3.3.3. | You must have a documented process for disclosure control of outputs from the TRE. | Mandatory | NA |
| 3.3.4. | You must have a process for assigning responsibility for output checking. | Mandatory | NA |

| | | | |
|---|---|---|---|
| 3.3.5. | You must have a documented policy for handling disclosure risks associated with any outputs that cannot be manually checked. | Mandatory | NA |
| 3.3.6 | You should have a statistical basis to guide the decisions of an output checker on the safety of outputs. | Recommended | 0 |
| 3.3.7 | You could create a semi-automated system for checks on common research outputs. | Optional | 2 |
| 3.3.8. | TRE outputs should be limited to the minimum required for sharing results of any analyses. | Recommended | NA |

**SATRE 3.4**

Score: 2/2

The Aridhia DRE has its own native metadata catalogue, FAIR Data Services. More information on FAIR can be found here.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 3.4.1. | You should provide a metadata catalogue of available datasets for users. | Recommended | 2 |

**SATRE 3.5**

Score: 6/6

The Aridhia DRE supports a variety of structured and unstructured data types, which are detailed in our service description and Knowledge Base. The DRE provides administrators with a variety of pre-defined security controls (e.g. system user roles), but also allows these to be configured to meet the needs of particular projects or customers.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 3.5.1. | You must be able to specify what categories of data your TRE is able to support. | Mandatory | 2 |
| 3.5.2. | Your TRE could support projects with differing security requirements through configurable security controls. | Optional | 2 |
| 3.5.3. | Your TRE could offer a pre-defined set of security control tiers. | Optional | 2 |

**SATRE 3.6**

Score: 4/4

The Aridhia DRE provides researchers with the ability to discover and understand data through dataset search, classification and efficient metadata browsing capabilities described via customisable dataset catalogues and associated dictionaries.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 3.6.1. | You should have a consistent and easily accessible meta-data data model or similar to describe what a data asset contains. | Recommended | 2 |
| 3.6.2. | You could provide summary, abstracted or synthetic data to researchers without exposing the underlying data set. | Optional | 2 |

**SATRE 3.7**

Score: 2/2

The FAIR Cohort Builder can be enabled on datasets held in the Aridhia DRE. This allows users to explore and summarise data before requesting access to it. The Cohort Builder also allows users to subset data, and only request those records that meet their project requirements.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 3.7.1. | You could provide an interface application for data consumers and data subjects to query elements of the data. | Optional | 2 |

**SATRE 3.8**

Score: 2/4

The Aridhia DRE allows users to hibernate workspaces that are no longer in use; these are maintained in a read-only state.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 3.8.1. | Archived data within the TRE should be read only. | Recommended | 2 |
| 3.8.2. | Long-term archives must be held in simple, standard formats to ensure accessibility. | Recommended | 0 |

**Supporting Capabilities and the Aridhia DRE:**

**Overall Score 30/30**

The Supporting Capabilities section of SATRE covers all the non-technical capabilities an organisation needs to successfully build and maintain a Trusted Research Environment, including project management, legal and financial support and the business processes required to ensure service continuity.

**SATRE 4.1**

Score 4/4

The Aridhia DRE is backed by a comprehensive business continuity plan. This is tested in quarterly business continuity exercises, monthly restore checks, and an annual full restore exercise.

| **Item** | **Statement** | **Importance** | **Score** |
|---|---|---|---|
| 4.1.1. | You should have a business continuity plan that includes consideration of loss of service for deployed TREs. | Recommended | 2 |
| 4.1.2. | You should regularly test the aspects of your business continuity plan concerning TREs, and have a process in place to iterate the plan if required. | Recommended | 2 |

**SATRE 4.2**

Score 2/2

All Aridhia customers have a dedicated project manager for the lifetime of their hub. The PM can assist in all aspects of hub management and connect users with other specialists within Aridhia.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 4.2.1. | You should ensure that all projects using your TRE have a named project manager. | Recommended | 2 |
| 4.2.2. | You should not give project managers direct access to the TRE. | Recommended | NA |

**SATRE 4.3**

Score 6/6

The features of the Aridhia DRE are documented in our service description documents. In addition, we provide users with a comprehensive Knowledge Base and online training courses. The customers' dedicated project manager can arrange bespoke training as required.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 4.3.1. | You must document all features of your TRE implementation. | Mandatory | 2 |
| 4.3.2. | You should have an education programme in place to upskill stakeholders in the use and management of your TRE. | Recommended | 2 |
| 4.3.3. | You should periodically carry out a training needs analysis (TNA) for all stakeholders included within your TRE provision. | Recommended | 2 |

**SATRE 4.4**

Score 6/6

Aridhia customers are provided with a full breakdown of their costs for use of the DRE, which can be tracked on a per project basis. All costs are reviewed by the Aridhia finance team and the assigned project manager to ensure value for money.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 4.4.1. | You must ensure that all projects using your TRE are aware of any associated costs and are able and willing to pay them. | Mandatory | 2 |
| 4.4.2. | You should be able to track the costs associated with each TRE project. | Recommended | 2 |
| 4.4.3. | You should have a process in place to ensure your TRE provision remains financially sustainable. | Recommended | NA |
| 4.4.4. | You should minimise the cost of your TRE infrastructure wherever possible | Recommended | 2 |

**SATRE 4.5**

Score 2/2

The Aridhia finance team track contract renewals for all suppliers.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 4.5.1. | You must identify any goods or services that will be needed to operate the TRE and ensure that a plan is in place to purchase them as needed. | Mandatory | 2 |

**SATRE 4.6**

Score 2/2

All users of the Aridhia DRE have the support of a full-time service desk team, and access to a customer portal to raise issues with them. The Service Desk targets a two-hour initial response time for all tickets.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 4.6.1. | Your TRE must have a team of Operators in place to support projects working with TREs. | Mandatory | 2 |

**SATRE 4.7**

Score 2/2

Customers have a variety of means of providing feedback on the Aridhia DRE. They can do so via the Service Desk portal, through their project manager, or in regular reviews with the DRE product team.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 4.7.1. | You should have a clear process in place for stakeholders to feedback on your TRE infrastructure. | Recommended | 2 |

**SATRE 4.8**

Score NA

No score is provided for this section. As a platform provider, Aridhia is not involved in the governance of individual projects.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 4.8.1. | All public engagement activities must include a range of perspectives and be inclusive (*optional for TREs without personal data). | Mandatory* | NA |
| 4.8.2. | Details of TRE operations, data available and projects which have accessed the data should be publicly available (*optional for TREs without personal data). | Mandatory* | NA |

| | | | |
|---|---|---|---|
| 4.8.3. | Members of the public should be included in TRE operations and/or oversight (*optional for TREs without personal data). | Mandatory* | NA |
| 4.8.4. | You should publicly share details of incidents, near misses, and mitigations in a timely fashion, in line with good practices for responsible disclosure. | Recommended | NA |

**SATRE 4.9**

Score 6/6

The Aridhia general council is consulted on all issues related to security, privacy, health and safety laws, regulations and policies. Our information security team can also provide advice to customers on data protection issues.

| Item | Statement | Importance | Score |
|---|---|---|---|
| 4.9.1. | You should identify areas where legal advice may be required and ensure that you have ready access to it. | Recommended | 2 |
| 4.9.2. | You should identify areas where advice on data protection issues may be required and ensure that you have ready access to it. | Recommended | 2 |
| 4.9.3. | You should identify who will be responsible for managing contracts related to the TRE. | Recommended | 2 |