WEST OF ENGLAND Combined Authority

Future Transport Zone: Transport Data Hub

Non-functional requirements
22/04/2022

3 Rivergate, Temple Quay, Bristol BS1 6EW

Contents

1. Introduction

1.1. The purpose of this document is to provide additional detail on the outcomes and identified non-functional requirements for the West of England Combined Authority Transport Data Hub. The document gives information on how we intend to deliver and manage the Transport Data Hub, our expected working relationship and the legislation, regulations and standards with which the delivery of the Transport Data Hub must comply.

1.2. Order of Precedence

This document will be incorporated into the Call-Off Contract as part of the Call-Off Special Terms. If anything in this document conflicts with Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables) or any other provisions of the Call-Off Contract dealing with data protection or information governance including but not limited to the Freedom of Information Act 2000, such schedule and other provisions shall have precedence.

2. Delivery Management

2.1. We want an innovative transport data solution that meets our needs now and provides a platform for future development beyond the Future Transport Zone (FTZ) trial period. Future options may include enhancement and extension of the initial functionality, and collaboration with external partners on innovation and research.

2.2. We want to be able to maintain a focus on delivering value at every stage. In providing the Transport Data Hub, you must adopt a collaborative approach, working alongside us, our consultant team, and our stakeholders to deliver a solution which provides maximum value to our stakeholders.

2.3. We want you to bring expertise in established ways of agile working, including appropriate tools and processes, and to work with us to tailor those practices to support agile delivery of the Transport Data Hub from inception to closedown.

2.4. We want you to be an active partner in the collaborative relationship, bringing constructive input and new ideas to the delivery.

2.5. We want significant flexibility in the development, deployment and future direction of the Transport Data Hub.

2.6. We want you to develop and agree a model for project roles and responsibilities, covering both delivery and operation of the solution. You will need to work collaboratively with stakeholders, including our existing supply chain. The model that you develop will need to identify boundaries and clearly allocate

responsibilities. We will work with you to agree these responsibilities with all stakeholders, in-line with existing services and contractual commitments.

2.7. We expect you to understand the needs of our project and propose an appropriately experienced team to deliver the work.

2.8. We want you to define the Product Owner role such that both we and you, as the supplier, are involved. We think that this is necessary to cover the technical, process and organisational knowledge needed to for an effective implementation.

2.9. We want to involve users and other stakeholders in the delivery process so that the solution meets their business requirements. This includes working with us to plan for business change so that required training, handover or resourcing happens at appropriate points in delivery.

2.10. We have completed some discovery activities and compiled a list of Use Cases that we would like to address with the Transport Data Hub. This has been done through initial engagement with our transport data users, other FTZ projects and unitary authorities. A summarised version is provided in the FTZ TDH Use Case document and a detailed version will be available at the next procurement stage. At this stage we are not able to specify the final functional requirements and want you to work collaboratively with us and users to define a prioritised backlog of User Stories to deliver the functionality to support our Use Cases. User Stories will be prioritised based on the value they bring.

2.11. We want to take a flexible approach to delivery, and additional User Stories may be introduced to address new functional priorities during the delivery phase. We will work with you to reprioritise the backlog to accommodate any changes.

2.12. We want to be engaged in the design of the solution and have set out our objectives, including performance, availability, maintainability, scalability, cost-effectiveness, and sustainability elsewhere in this document. We want you to include our team in the development of your designs so that we can work collaboratively to align the solution with our objectives. We want you to develop the architecture for the solution following best practice methods such as TOGAF, including implementing reusable capabilities where appropriate.

2.13. We want you to work collaboratively with our current infrastructure provider to implement the technical solution within our existing managed Azure cloud environment.

2.14. We want to deliver a Minimum Viable Product (MVP) for the Transport Data Hub, which provides useful functionality and recognises early value for high-priority Use Cases.

2.15. Once the MVP has been delivered, we want to be able to work independently to introduce new datasets into the solution and implement data analytics alongside your development. We want you to support this in your delivery approach, and knowledge transfer to our teams and potentially to third parties.

2.16. We want you to develop and agree processes to enable the iterative delivery of new functionality into live testing, approval and release of new functionality. We want you to adopt industry best practices such as DevOps and DataOps where this is appropriate.

2.17. We want you to be able to demonstrate progress against key milestones and spend profile against your commercial offer, by roles and time, so that we can monitor delivery timescales and budget. Progress reporting should align to agile methodology and emphasis should be placed on dashboard-style reporting.

2.18. We want to be able to monitor and evaluate the impact of the Transport Data Hub as capability and capacity is increased. We will need to extract and report on appropriate performance parameters to do this.

2.19. We may want to audit any aspect of your delivery of this work and will require your cooperation and support to complete this activity.

2.20. We want to follow Service Management best practice, such as ITIL, and expect you to implement and integrate appropriate processes to support this.

2.21. We want to collaboratively manage risk and expect you to proactively identify and mitigate risks and engage with our project risk management protocols.

2.22. We want you to adopt a robust process for logging, tracking and resolving issues, defining who can raise issues, response times, cost implications, approvals and closure.

2.23. We want you to facilitate a smooth handover to us at the end of the contract, covering the records, processes and knowledge required to operate, maintain and extend the solution.

2.24. We want comprehensive records to be created for the Transport Data Hub project, including designs, test activities, configuration details, and operational process documentation. We want these to be accessible to us and nominated stakeholders during project delivery and to be transferred to us no later than the end of the project.

2.25. We will own all Intellectual Property Rights (IPR) arising from the delivery of this project but will grant you the right to use this IPR to the extent necessary to enable you to perform your obligations under the contract including in respect of maintenance and support.

2.26. You must confirm that all components of the solution are appropriately owned or licensed during the project. We will need to confirm that all components are appropriately licensed to us following the end of the project. You must:

2.26.1. Identify all necessary licences for third party components including COTS Software and third party software that is not COTS Software

2.26.2. License any components that you have developed outside the project that we need to use for it, and

2.26.3. Grant us the right to use all components that have been developed in this project at no additional cost that we do not own.

2.27. We want to share progress, best practice and learning with the FTZ community, national bodies, regional and local authorities in the UK and wider industry and expect your support in this.

3. Operation, Management, Maintenance, and Support of the Solution

3.1. We want the solution to consistently meet the expectations of our users and want you to implement robust management and maintenance practices aligned to ITIL Service Operation processes. We want all suppliers to collaborate in the best interest of the Combined Authority.

3.2. We want you to take a proactive approach to management and maintenance activities, including:

3.2.1 Supplier service reviews;

3.2.2 Capacity management;

3.2.3 Security monitoring;

3.2.4 Incident management;

3.2.5 Configuration and change management;

3.2.6 Patch and software version management (including network appliances if relevant);

3.2.7 Access management; and

3.2.8 Service continuity management.

3.3. We want you provide support for users and other stakeholders once the MVP is live. We want this support to be provided via email and phone during our Core Business

Hours (08:00-18:00, Monday-Friday) and we will work with you to agree detailed availability SLAs and measurement methods.

3.4. We will work with you to agree reasonable SLAs, KPIs and metrics for all processes and support activities.

3.5. We want you to design a solution to:

- Be appropriately resilient;
- Be maintainable; and
- Enable effective security management.

3.6. We want to be kept informed about management and maintenance activities, such as through dashboards or reports. We want you to plan maintenance activities and share that plan with us. Planned changes will follow change control and changes to be deployed in Production will be subject to approval by us. We will agree a procedure for emergency changes with you.

3.7. Planned maintenance should be conducted outside core business hours where it will affect the functionality or availability of the solution. We may require you to modify maintenance procedures or delay maintenance activities to reduce the impact on our users.

3.8. We will agree procedures for reactive maintenance with you, including incidents that occur outside core business hours. We agree arrangements for regular service reviews with you.

3.9. We expect you to develop a plan of future maintenance and engage with our stakeholders to finalise it.

4 Testing

4.1 We must verify that all deliverables meet our needs as defined by these requirements and are reasonably free from defects to our satisfaction. We want you to evidence this through testing and other demonstrations of compliance. Key stakeholders will be involved from the beginning to the final 'sign off' of the requirement.

4.2 We want to understand and influence the test approach and want you to produce and agree a test strategy with us that will cover testing of iterative implementation and configuration activities, and system-wide testing at key points in the delivery.

4.3 We want to take a risk-based approach to testing so that test activities provide an appropriate level of rigour based on factors such as the impact of non-compliance and cost to rework (which we expect you to bear).

4.4 We want to take a collaborative approach to testing deliverables to provide confidence that the requirements have been effectively verified and that defects

have been identified. We will work with you to agree defect severity classifications and thresholds for acceptance.

4.5 We want to you conduct testing to cover all aspects of the delivery, which may include the following types of testing:

4.5.1 Unit testing to verify that subsystems, modules and components meet the design requirements.

4.5.2 Interface Testing to verify that internal and external interfaces (including APIs) meet the relevant requirements and specifications.

4.5.3 Integration Testing to verify that subsystems, modules and components successful integrate to deliver the required functionality.

4.5.4 Whole system testing to verify that the complete system delivers the required functionality (based on functional areas or end-to-end delivery of processes).

4.5.5 Infrastructure testing to verify that supporting infrastructure delivers the required functionality and performance.

4.5.6 Accessibility Testing to verify that User Interfaces meet Accessibility Requirements

4.5.7 User Acceptance Testing (UAT) to enable the Customer to satisfy themselves that the required functionality has been delivered and that non-functional requirements, such as useability are met.

4.5.8 Business Logic Testing to verify the business rules and transform logic for the ETL/transformation process to ensure data completeness and accuracy

4.5.9 Performance Testing to verify that response times, latency and throughput meet the relevant requirements. This may include stress testing to verify peak load requirements can be met

4.5.10 Soak testing to verify that the solution of solution component is stable over an extended period.

4.5.11 Resilience Testing to verify that resilience and redundancy features such as backups and redundant infrastructure function as intended.

4.5.12 Security Testing to verify that the cybersecurity requirements are met. This will include testing at key points in the delivery and regular pen testing of the solution.

4.5.13 Regression Testing to verify that changes to the solution do not break existing functionality or degrade performance.

4.5.14 Data Quality Testing to verify accuracy, completeness, and consistency of data. This will include defining specific data quality metrics, identifying baselines, and conducting tests to identify any gaps to the baselines.

4.5.15 Business Continuity Testing to verify that contingency plans are in place to ensure that the processes and systems used by the Supplier to Support the Solution are resilient to common issues such as staff absence or equipment failure.

4.5.16 Operational Process Testing to verify that operational and maintenance processes such as promotion of changes between environments function correctly.

4.5.17 In-service Testing and Ongoing Monitoring to verify that requirements and SLAs such as availability are met on an on-going basis.

4.5.18 Compliance Validation to verify requirements that cannot feasibly be met through testing such as scalability via inspection of deliverables such as designs.

4.6 We want to be kept informed of progress of testing and defects such as through dashboards or reports.

4.7 We would like test activity to be conducted efficiently and want you to implement industry standard and best-practice testing methods such as test automation where appropriate.

4.8 We need a technology solution that will support and enable testing during delivery and operation.

4.9 We want you to work with us to develop a target operating model and define requirements that the solution will need to meet in order to realise this.

5 Availability

5.1 We want to provide a good user experience and want a solution that is available when required by our stakeholders. We want you to deliver and operate a solution that achieves this aim.

5.2 We want a solution that is resilient to unexpected events and want you to put in place Business Continuity and Disaster Recovery (BCDR) arrangements for the solution and operational processes. We also want to have BCDR arrangements in place for your own business systems and processes.

5.3 Our initial Use Cases are non-critical but we anticipate that we will implement Business Critical Use Cases as we extend the Transport Data Hub and want you to deliver and operate a solution to achieve these which deliver 99.9% availability of all functionality within Core Business Hours (08:00-18:00) excluding planned outages, measured over a rolling 30 day period (i.e. no more than 44 minutes of unplanned downtime per month). We may consider proposals that provide reduced availability for some functionality where that meets the requirements of relevant Use Cases and provides other benefits aligned to our objectives.

5.4 We do not want to lose data due to a technology failure or other issues with the solution and want you to build resilience into the solution to achieve this.

5.5 We want to ensure that data we ingest is complete and want to you agree and implement arrangements, which may be a combination of technology and process, with data providers to ensure that any gaps caused by unavailability on either side are remediated promptly. We expect to be engaged in this agreement.

5.6 We want to have visibility of the availability of the system and want you to provide access to such information, in real-time, in an accessible format such as a dashboard or report.

6 Cost effectiveness, performance and scalability requirements

6.1 We need a solution that is cost effective and expect you to consider ongoing operational costs when developing the solution.

6.2 We want the Transport Data Hub to provide a good user experience for all of the Use Cases identified in the backlog. We will work with you during the early part of the project and throughout the delivery of Use Cases to agree what a good user experience looks like.

6.3 We want our solution to handle growth in the number of users and data for the Use Cases identified in the backlog. We expect the solution to provide headroom for growth in the short to medium term and a cost-effective route to support further growth in future.

6.4 We want the solution to provide a suitable platform for future development and expect that architecture will be designed to provide a cost-effective route to support future innovation and new use case.

7 Cybersecurity

7.1 We must comply with cybersecurity requirements and apply best practices to the integrity, confidentiality, and availability of the solution. We want you to enable us to do this by implementing a solution and operating processes that are secure by design and follow industry best practices such as NCSC's 10 principles.

7.2 We must comply with NIS-D standards and want the solution you deliver to implement the NIS-D objectives:

- Managing security risk
- Protecting against cyber attack
- Detecting cyber security events

- Minimising the impact of cyber security incidents.

7.3 We want the solution to be compliant with requirements of the Public Services Network (PSN) (https://www.gov.uk/government/groups/public-services-network#psn- compliant-services) or the successor PSN set of requirements.

7.4 We want you to follow industry best practices in your organisation. You must demonstrate this through accreditation under a recognised scheme such as cyber essentials plus or ISO27001.

7.5 We want our data to be appropriately protected in transit and at rest. We expect you to take a risk-based approach to deliver appropriate encryption, access control and monitoring.

7.6 We want you to appropriately control and mange access to the solution, including:

- Access by the developer to deliver the system
- Internal access to the system
- External access to the system

7.7 We want you to work collaboratively with our IT systems providers and supply chain partners so that shared systems and processes are secure.

7.8 We want to be open, collaborative and proactive in your approach to all security activities including incident handling.

7.9 The solution should be secure. We want you to conduct regular, independent PEN testing using a CREST, TIGER or CHECK-accredited tester prior to deployment of the MVP and every 12 months following deployment. You must address any issues identified by the PEN testing.

7.10 We require the supplier to comply with the following:

7.10.1 UK GDPR and the Data Protection Act 2018

7.10.2 ISO27001 certification

7.10.3 PEN test to be CREST, TIGER or CHECK-accredited

7.10.4 Cyber essentials plus

7.10.5 NIS-D and DfT's Implementation guidance

7.10.6

7.11.2

7.12 We require the solution to be designed to support effective security management and we expect the supplier to be proactive in their security management at the solution.

8 Information Rights

8.1 We must handle, store and process information in a secure, compliant, legal and purposeful manner. We implement information rights management to enable us to do this.

8.2 You will handle our data within our systems and you must:

8.2.1 Work in compliance with our information rights policies, and

8.2.2 Comply with relevant requirements from the Freedom of Information Act (FOIA), UK GDPR and the Data Protection Act 2018.

8.3 When developing the solution and processes we want you to give due consideration to the following:

- What data is held;
- Where it is held;
- Where it is stored;
- How it is used;
- Its sensitive categories and classifications; and
- How it is archived and disposed of.

8.4 We expect you to implement processes so that a secure approach is taken to the above phases and associated risks are logged and addressed.

8.5 We want you to design a solution which will support information rights management activity and enable us to comply with our obligations under the FOIA, UK GDPR and Data Protection Act 2018.

9 Compliance

9.1 We must comply with all applicable legislation, standards and regulations through the delivery of the project and operational life of the solution. We want you to support us in identifying and delivering our compliance obligations.

9.2 We expect you to understand the legislation, standards and regulations referred to in this document and to identify and communicate to us applicable standards or regulations that have not been identified but with which this project needs to comply.

9.3 We must be able to provide evidence that we have met our compliance obligations. We expect you to demonstrate that compliance requirements were satisfied and maintained throughout the delivery of the project.

9.4 Please note that this project is not required to follow Government Digital Services processes or approval gateways.

9.5 You must comply with all applicable regulations relating to the delivery of this project including but not limited to the following:

9.5.1 Freedom of Information Act 2000 (FOIA)

9.5.2 UK GDPR and the Data Protection Act 2018

9.5.3 NIS-D and DfT's Implementation guidance

9.5.4 PEN testing must be conducted using a CREST, TIGER or CHECK-accredited tester

9.5.5 You will be accredited under a recognised scheme such as cyber essentials plus or ISO27001

9.8 We want you to align with the best practice as described by the following:

9.5.1 NCSC 10 principles

9.5.2 Public Service Network requirements (https://www.gov.uk/government/groups/public-services-network#psn-compliant-services) or the successor PSN set of requirements

9.5.3 You service management approach must align with ITIL

10 Sustainability, carbon and corporate social responsibility

10.1 Our objective is for the Combined Authority to be carbon zero by 2030. We consider the environmental impact of all of our projects and account for in our designs. For more information about our sustainability ambitions please refer to the Climate Emergency Action Plan: [https://westofengland-ca.moderngov.co.uk/documents/s2200/CE%20Action%20Plan.pdf]

10.2 We want to work with suppliers who operate in an environmentally friendly and sustainable manner and whose own targets are aligned with ours. We expect you to meet the standards of the DOS framework and follow good environmental management practice, such as those set out in ISO4001.

10.3 We want a technology solution that is energy efficient and expect you to work with us to design a solution to meet this goal.

10.4 The Combined Authority aim to support creation of social value through all the projects we do. We want you to support our social value objective and do what you can to add value by considering the following:

- Direct or indirect investment into the project e.g. in terms of development time, marketing support;

- Social value benefits, including local employment, and upskilling local communities with digital skills;
- Including a local SME within your consortium or supply chain; and
- Support and make a positive contribution to the equalities, inclusion and inclusive growth agenda in the region.