**Technical Requirements**

|  |  |  |
| --- | --- | --- |
| **Reference** | **Theme** | **Requirement** |
| Competition Component | | |
| Info |  | **Competition data** includes: Tender (including auction and DPS qualification where appropriate), Proposal, and links to agreement information.  See Annex 2 Technical Specification for further definitions. |
| 01 | Tech Spec | The competition data MUST be made available by an API using standard web protocols such as JSON REST |
| 02 | Tech Spec | The supplier SHOULD be able to provide OCDS compatible extracts |
| 03 | Tech Spec | The solution SHOULD make it possible to link to or import content from external agreement document elements such as linking or loading Quality Questions from items within standard questionnaires. |
| 04 | Tech Spec | The solution SHOULD make it be possible to create or update content in external agreement document elements, such as completing supplier details in call-off schedules. |

|  |  |  |
| --- | --- | --- |
| **Reference** | **Theme** | **Requirement** |
| Evaluation and Award Component | | |
| Info |  | **Evaluation data** includes Evaluation Responses, Evaluator details, and Evaluation Tasks, plus links to relevant proposal data from Competition.  See Technical Spec for further definitions. |
| 01 | Tech Spec | Evaluation data MUST be made available by an API using standard web protocols such as JSON REST. |
| 02 | Tech Spec | The supplier SHOULD be able to provide OCDS (Open Contracting Data Standard: Documentation)  Compatible extracts where appropriate. |
| 03 | Tech Spec | Evaluation and supporting competition data MUST be version controlled. |

|  |  |  |
| --- | --- | --- |
| **Reference** | **Theme** | **Requirement** |
| User Registration and Access Control | | |
| Info | Tech Spec | All users of the solution will be authenticated by third party identity providers who act as the Authority on behalf of the Vendor. At the time of writing these are in the case of suppliers: SID4GOV and buyers: Google Authentication Service and Salesforce. |
| 02 | Tech Spec | The solution MUST support SAML2 and/or OpenID Connect identity assertions and MUST NOT require independent authentication and registration. |
| 03 | Tech Spec | The solution SHOULD be able to ingest common supplier qualification documents from our appointed registration sources such as SID4GOV. This is required so that qualification questions and common answers will not have to be repeatedly answered by suppliers across Proposals. |

|  |  |  |
| --- | --- | --- |
| **Reference** | **Theme** | **Requirement** |
| Agreement Records and Party Records | | |
| 01 | Tech Spec | Solutions SHOULD refer to and update authority summary details of agreements and parties in Salesforce via APIs using standard web protocols such as JSON REST. Interface details will be agreed later.  Data export / import processes SHOULD be considered as a fall back if API mechanisms can’t be built on those processes. |

|  |  |  |
| --- | --- | --- |
| **Reference** | **Theme** | **Requirement** |
| Document store | | |
| 01 | Tech Spec | The authority stores documents in Google Drive. Amazon S3 also will also be used for application document storage. Solutions SHOULD read and write data to the document stores via relevant web APIs. |

|  |  |  |
| --- | --- | --- |
| **Reference** | **Theme** | **Requirement** |
| Strategic Alignment | | |
| 01 | Tech Spec | Solutions should comply with the CCS overarching Annex 3 Sourcing Services Design. |
| 02 | Tech Spec | All components SHOULD offer web APIs ideally supporting REST JSON interfaces.  Messaging MAY be by email but all auditable interactions SHOULD be by secured web interfaces to be agreed. |

|  |  |  |
| --- | --- | --- |
| **Reference** | **Theme** | **Requirement** |
| Technical quality requirements | | |
| 01 | Tech Spec | Solutions should comply with the CCS overarching Annex 3 Sourcing Services Design. |
| 02 | Tech Spec | Solutions and solution providers MUST demonstrably conform to UK Government standards:   |  |  | | --- | --- | | Technology Code of Practice | https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice | | GOV.UK Design Standard | https://www.gov.uk/service-manual/service-standard | | Cloud Security Principles | https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles | | Security Design Principles for Digital Services | https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main | | Protecting Bulk Personal Data | https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main | |

|  |  |  |
| --- | --- | --- |
| **Reference** | **Theme** | **Requirement** |
| Availability requirements | | |
| 01 | Tech Spec | **Total availability**: the solution MUST be available 24 by seven with an availability of 99.95%, excepting agreed maintenance outages. |
| 02 | Tech Spec | **Maintenance and core hours**: planned maintenance MUST occur outside core hours of 8am to 6pm Monday to Friday UK time. |
| 03 | Tech Spec | **Recovery Time Objective**: Services MUST be restored after unintentional outage within 4 hours of any one incident and also no more than 30 minutes beyond any underlying cloud operator outage, whichever is smaller. There must be an aggregate annual total of no more than .05% outage (4 hours 22.8 minutes). Exceeding these outages will incur service credits. |
| 04 | Tech Spec | **Recovery Point Objective**: Each web page SHOULD automatically save significant page content where JavaScript is available to avoid data loss. Once web transactions have been made, there MUST NOT be more than 5 minutes of work lost. |
| 05 | Tech Spec | **Response time**: 95% of requests to *core pages/actions* respond within 1 second. 95% of agreed *non-core pages/actions* respond within 1 minute.  For clarity - The solution provider and authority to agree on core and non-core pages, but broad expectation is that all workflow data entry activities are core, whereas document generating, analysis and reporting actions are non-core. Responses which exceed the required responsiveness should be logged. A performance report should be provided to the authority. Where performance goals are not met the provider must design and enact a remediation plan and service credits may apply. Even when performance goals are met if non performing pages are impacting user performance, for example pages taking excessive time even where 95% are within time, a performance plan should be put in place to mitigate the impact. |
| 06 | Tech Spec | **Disaster recovery**: solution provider shall have a system recovery mode in case of total loss of cloud region within two days, which will be activated if the authority agrees the cloud service provider will not restore service within an acceptable time frame. |
| 07 | Tech Spec | **Repeated failure of underlying cloud service provider**: if cloud service provider breaches 99.95% availability within a year the authority may require the solution provider to plan to migrate to another cloud service provider. |
| info | Tech Spec | **Service credits chain**: service credits apply to solution provider. These will defined at contract.  Downward call of service credits from cloud service providers are the solution provider’s responsibility. |

|  |  |  |
| --- | --- | --- |
| **Reference** | **Theme** | **Requirement** |
| Confidentiality, integrity and data protection | | |
| 01 | Tech Spec | Data MUST be resident in data centers in the European Economic Area. |
| 02 | Tech Spec | Data MUST be processed and stored in accordance with Data Protection Act 2018 and thus General Data Protection Regulations [GDPR] regulations. |
| 03 | Tech Spec | At the authority’s request, data processing and storage MUST be moved to UK public cloud residency within six months of activation of request at solution providers cost. |
| 04 | Tech Spec | All personal data SHOULD be synchronised via APIs to allow coordination with the authority’s identity records. Personally identifiable fields must be marked and available for reporting and management according to GDPR regulations |
| 05 | Tech Spec | All data MUST be handled in line with Cloud Security Principles as above.  Specifically measures must be taken to protect against   1. Leaking of commercially sensitive bid data prior to publishing 2. Malicious or accidental modification of any commercial data, whether published or not |

|  |  |  |
| --- | --- | --- |
| **Reference** | **Theme** | **Requirement** |
| Updates | | |
| 01 | Tech Spec | **Patches**: The service MUST be updated to provide security and bug fixes in the shortest reasonable time not impacting availability requirements. Such patches MUST be thoroughly tested prior to release. Rollback options MUST be available. The authority MUST be informed of system changes at the time of release. Any non-trivial risk on a patch SHOULD be notified to the authority two days prior to release and contingency plans should be in place. |
| 02 | Tech Spec | **Functional impact**: Small functional service updates may be made at any time so long as the usability of the updates is obvious, is a small change and has been user tested with users from the authority or similar organisations. Such changes should be self-evident and not require formal training. Larger changes that may not be obvious MUST be notified to the authority at least seven days before release and should have been user tested with the authority. A/B testing modes are preferred in this case so that functional changes can be released to small agreed subsets of authority staff for user testing. |
| 03 | Tech Spec | **Technical interfaces**: APIs should distinguish between minor and major versions, in line with semantic versioning standards such as https://semver.org. Minor version changes should be backwards compatible. Major version changes should be offered in parallel and older versions should not be retired until providing the authority with at least three months notice. |

|  |  |  |
| --- | --- | --- |
| **Reference** | **Theme** | **Requirement** |
| Optional Collaborative Agreement Design Component | | |
| 01 | Tech Spec | The authority wishes to reduce reworking of content from document to document, platform to platform.  Elements of an agreement SHOULD be linkable and importable into competition processes and other components so as to reduce or remove ‘re keying. For example it should be possible to link Questionnaire templates from standard agreement schedules into various competition processes, question by question, by some API or import/export process, |
| 02 | Tech Spec | The system SHOULD have the capability to allow editing the content of an agreement in a modular referenced structures as distinct from conventional collaborative document management. This will be separate from the process of rendering the agreement to, for instance, PDF documents. |
| 03 | Tech Spec | Other ways in which the elements of an agreement document can be cross referenced and made available in competition will be considered, such as template based content substitution and document mark-up based data extraction. |