Technical Specification for eSourcing

[**Conceptual Design**](#_nwu5pvrfk0s8)1

[Main solution components](#_a2juqwt51net) 1

[Collaborative Agreement Design Component](#_jr40baq7ox6k) 2

[Agreement](#_y4wyx2ltmga3) 3

[Competition Component](#_7k36jdd0in4a) 4

[Tender](#_jif58cb2d2cn) 4

[Proposal](#_gztx3y8l61l6) 4

[Evaluation and Award Component](#_4xzh0moflgjh) 5

[User Registration and Access Control](#_kof19pl01nnm) 5

[Agreement Records and Party Records](#_h4y8twxww5yc) 5

[Document store](#_1x711nbzdefs) 6

[Summary notes on data model](#_agcwsk7di30) 6

[Strategic Alignment](#_yd0s3rw1ue4q) 6

[Interfaces and technical standards](#_cdgpi41atffh) 6

[Web Site](#_ytmxpxvo7yr) 6

[**Technical quality requirements**](#_x8kfrn3djnow)7

[Government standards and principles](#_tb5rd7icyzy6) 7

[Availability requirements](#_um406p4b63p8) 7

[Confidentiality, integrity and data protection](#_smcs4ikrkmcw) 8

[Updates](#_zao5ljz511j) 8

# Conceptual Design

Figures follow UML 2.5 [<http://www.omg.org/spec/UML/2.5>] class and component diagram formats.

## Main solution components

The solution should be in the form of two conceptual components, one for ‘competition’ and one for ‘evaluation and award’, which may be supplied individually or together. The solution MAY include an optional third component for agreement design. A specialised eAuction component MAY be supplied separately or as part of the solution.

Solutions should be able to read and write data via API interfaces using web standard interfaces.

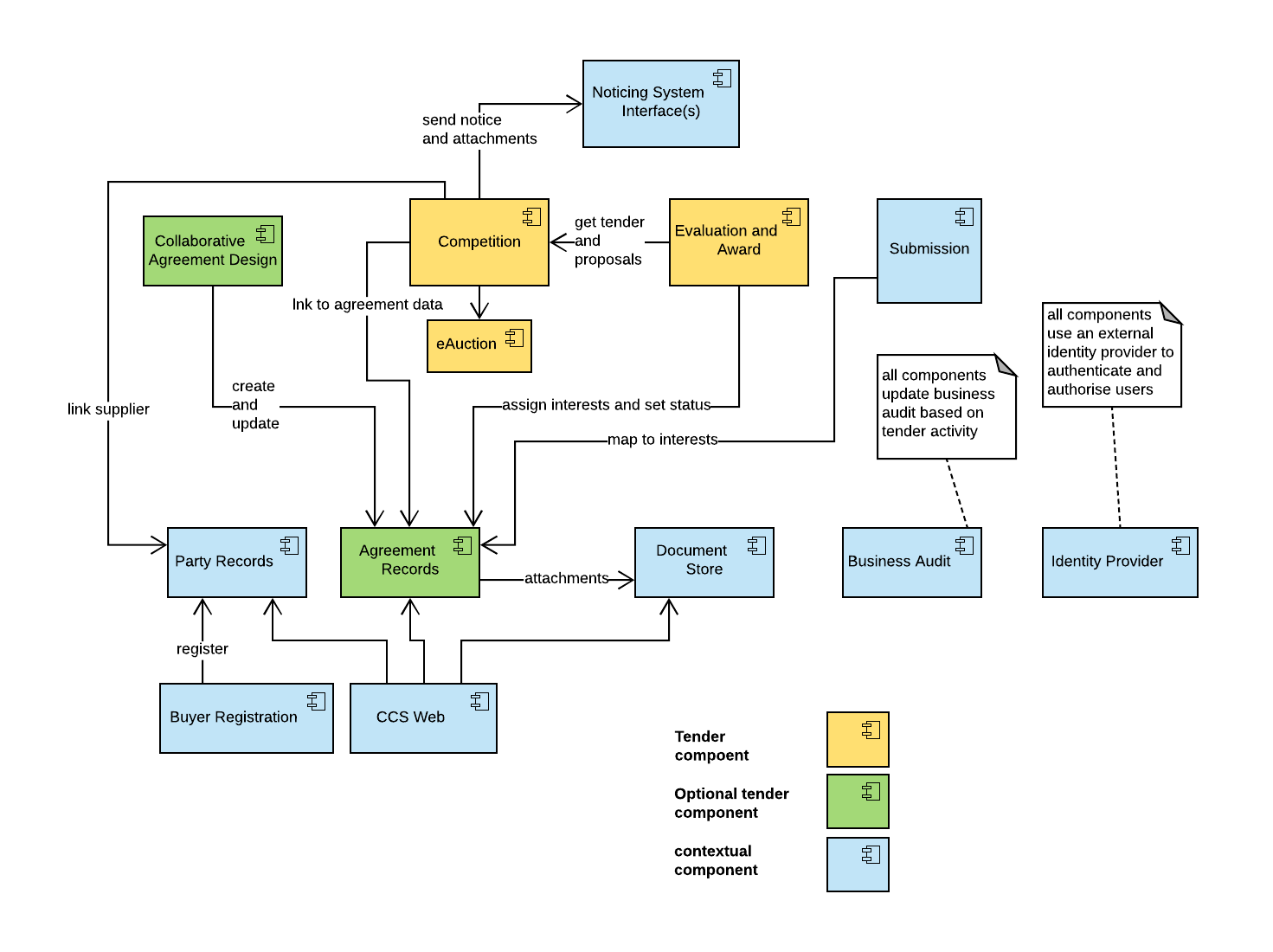


Figure: conceptual solution components and context

### Collaborative Agreement Design Component

An **optional** component allowing arbitrary agreements (such as framework contracts and call-offs) to be created, edited, collaborated around and linked to.

Agreement content MUST be version controlled.

Elements of the agreement SHOULD be linkable and importable into competition processes and other components so as to reduce or remove ‘rekeying’. 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, rather than expect users to manually rekey or update the questions. Likewise it should be possible to complete a Schedule from a template including, for example, details of awarded suppliers, rather than expect users to create copies of templates and manually update entries.

The system SHOULD allow editing the content of an agreement, separate from the process of rendering the agreement to, for instance, PDF documents. This capability is distinct from conventional collaborative document management because the agreement structures are modular and referenceable, not freeform documents. We appreciate this is a specialist need and hence the requirement is optional.

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.

#### Agreement

Agreement is a general term for all contract, framework, call-off, Dynamic Purchasing System agreement or other structured description of an agreement between two parties.

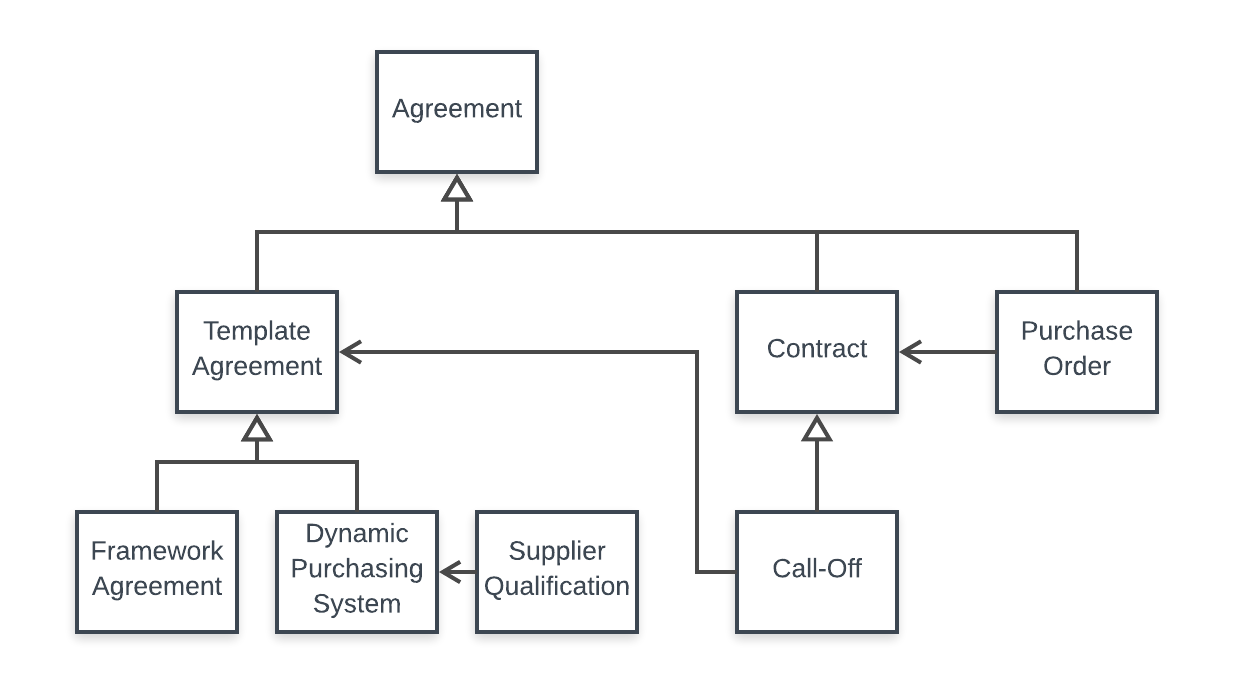


Figure: kinds of agreements

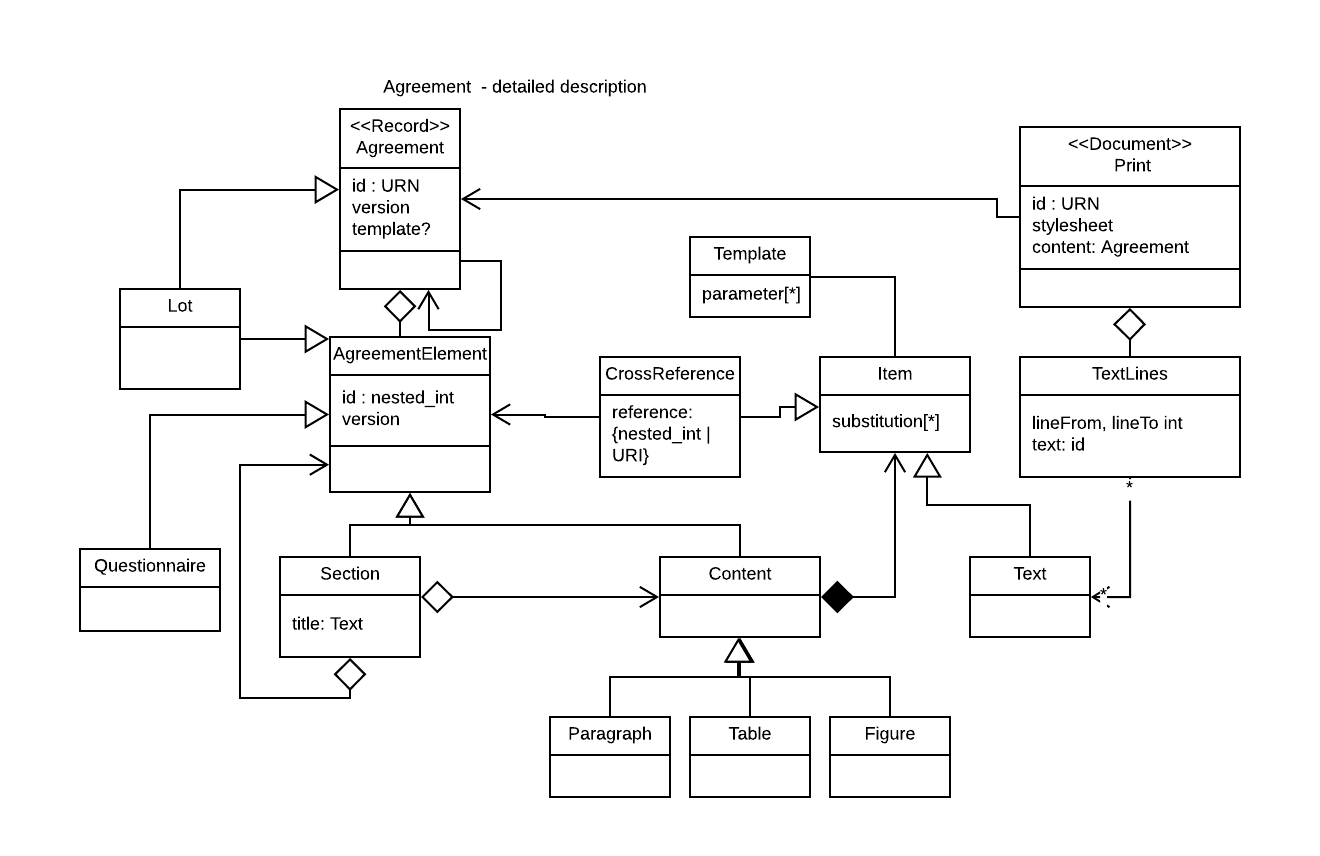


Figure: Agreements are ideally structured semantic content, not just documents

### Competition Component

The Competition component handles creating the tender and interacting with bidders according to a prescribed sourcing procedure. Tender content MUST be made available by an API using standard web protocols such as JSON REST. The solution SHOULD be able to provide OCDS compatible extracts. Tender and supporting competition data MUST be version controlled.

Whether a collaborative agreement design tool component is included, it SHOULD be possible to link to or import content from external agreement document elements such as linking or loading Quality Questions from items within standard questionnaires. It also SHOULD be possible to create or update content in external agreement document elements such as completing supplier details in call-off schedules and the like. In other words the Competition component’s interactive content should be linkable or updatable to and from external agreement data in order to prevent manual re-keying effort and error.

#### Tender

The data relating to going to market with an Agreement.

#### Proposal

A bidder proposing an interest in a Tender. In the case of a DPS a proposal is used to handle qualifying suppliers on to a DPS. In the case of Auctions the Tender represents the auction requirements, or there is a larger tender that includes an auction as a part of the competition process.

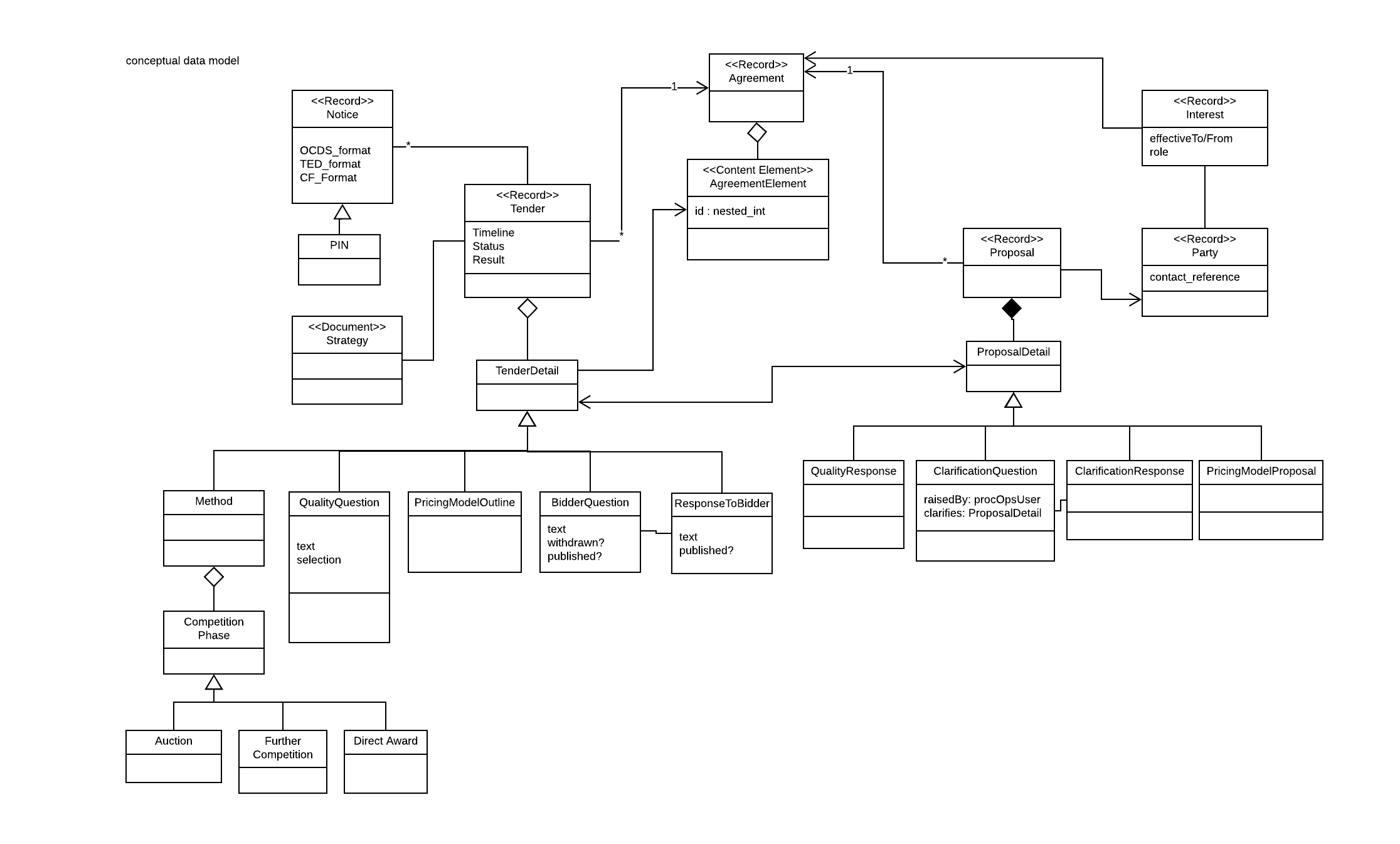


Figure - competition model

### Evaluation and Award Component

The Evaluation and Award Component handles data and tasks evaluating bidder proposals. Evaluation content MUST be made available by an API using standard web protocols such as JSON REST. The solution SHOULD be able to provide OCDS compatible extracts. Evaluation and supporting competition data MUST be version controlled.

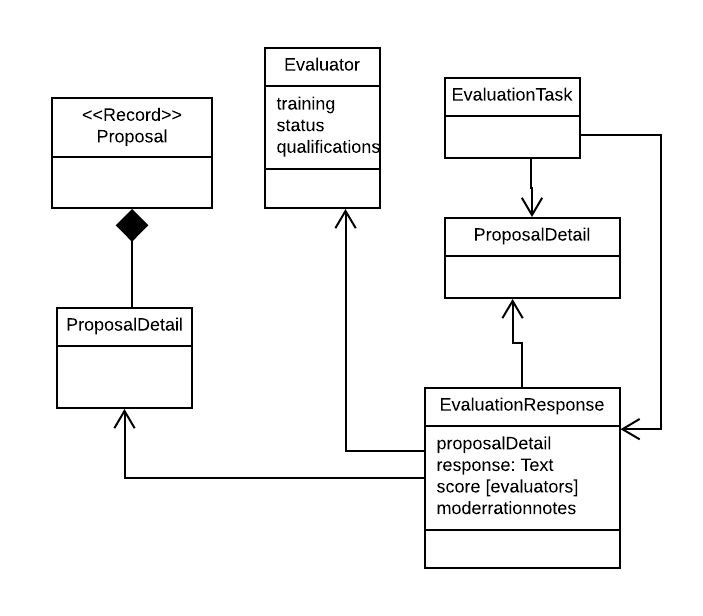


Figure - evaluation conceptual data

### User Registration and Access Control

All users of the solution will be authenticated in Authority provided identity provider services. Currently these are SID4GOV for suppliers, and Google Authentication Service for Authority actors, and SID4GOV or other identity provider for Buyers.

The solution must support SAML2 and/or OpenID Connect identity assertions and MUST NOT require independent authentication and registration.

The solution SHOULD be able to consume common supplier qualification documents from registration sources such as SID4GOV such that certain qualification questions and common answers do not have to be repeatedly answered across Proposals.

The system MUST properly use the asserted user and organisation IDs for internal storage and reference to APIs against User and Party records.

The system MUST properly use the asserted user identity assertion when determining user groups, roles and access control. Specific role based authorisation will be performed within the system.

### Agreement Records and Party Records

The authority stores summary details of agreements and parties in Salesforce. Solutions SHOULD refer to and update these data records via APIs, details of which are to be agreed. Data export / import processes may be considered as a fall back if API mechanisms can be built on those processes.

### Document store

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.

### Summary notes on data model

From the components above we have is a conceptual model expressing processing and interfacing requirements. Solutions should comply with the model conceptually via some mapping - it is not necessary to literally support each entity type by name.

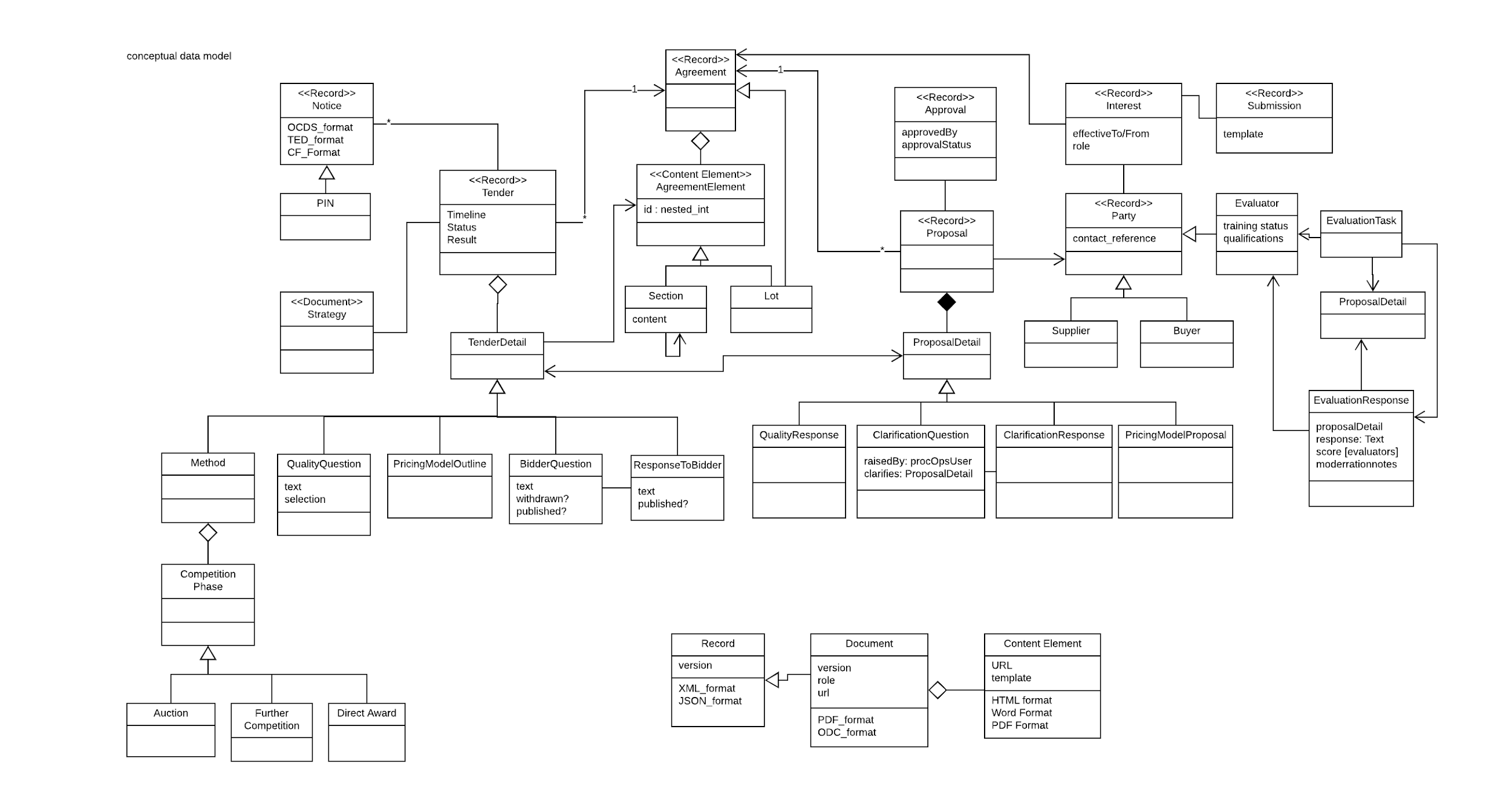


Figure: summary data model

## Strategic Alignment

Solutions should comply with the CCS overarching Copy Sourcing Services Design

## Interfaces and technical standards

All components SHOULD offer web APIs ideally supporting REST JSON interfaces.

Notification of messages MAY be by email but all auditable interactions MUST be by secured web interfaces.

Email use should comply with [Guidance for Securing government email](https://www.gov.uk/guidance/securing-government-email).

## Web Site

Service should be offered on e-sourcing.crowncommercial.gov.uk.

Service should [comply with CCS style guides and patterns](https://github.com/Crown-Commercial-Service/CCS-Architecture-Decision-Records/blob/master/doc/adr/0002-use-a-consistent-user-experience.md).

# Technical quality requirements

## Government standards and principles

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 |

These principles apply to the solution offered, the behaviours and practices of the solution provider, and all their subcontractors and partners.

## Availability requirements

In accordance with Technology Code of Practice solutions are expected to be supplied in commodity cloud data centres and provided as Software as a Service solutions where the Authority is not required to administer or patch the solutions. In line with this we expect solution providers to give availability assurances in line with commodity cloud providers at an availability of 99.95%. We expect solution providers to return the service to normal operations *within 30 minutes* of underlying cloud service provider availability.

**Total availability**: the solution MUST be available 24 by seven with an availability of 99.95%, excepting agreed maintenance outages.

**Maintenance and core hours**: planned maintenance MUST occur outside core hours of 8am to 6pm Monday to Friday UK time.

**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 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.

**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.

**Response time**: 95% of requests to *core pages/actions* respond within 1 second. 95% of agreed *non-core pages/actions* respond within 1 minute. 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.

**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.

**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.

**Service credits chain**: service credits apply to solution provider. Downward call of service credits from cloud service provider are the solution provider’s responsibility.

## Confidentiality, integrity and data protection

Data MUST be resident in data centers in the European Economic Area.

Data MUST be processed and stored in accordance with Data Protection Act 2018 and thus General Data Protection Regulations [GDPR] regulations.

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.

Personally identifiable fields must be marked and available for reporting and management according to GDPR regulations. All personal data SHOULD be synchronised via APIs to allow coordination with the authority’s identity records.

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

## Updates

In line with Technology Code of Practice we expect services to be continuously iterated and improved. We expect reasonable engagement in functional requirements and user testing of changes. We need reasonable notice of larger changes and need to be able to object to changes that substantially impact the effectiveness of the service.

**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.

**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.

**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.