

Capita Tendering AI

Service Definition

G-Cloud 15



Contents

1 Overview 1

2 Service Features 4

3 Service Benefits 5

4 Service Scope 6

5 Disclaimer 8

1 Overview

Provide a short word plain-English summary describing what the service is, who it is for, and the problem it solves. Avoid marketing language and use terminology that buyers are likely to recognise (i.e. not overly technical).

Advice from CCS is for this to cover:

- what the service is
- the levels of data backup and restore, and disaster recovery you'll provide, such as business continuity and disaster recovery plans
- any onboarding and offboarding support you provide
- service constraints like maintenance windows or the level of customisation allowed
- service levels like performance, availability and support hours
- after sales support
- any technical requirements
- outage and maintenance management
- hosting options and locations
- access to data (upon exit)
- security
- any ancillary services

Tender evaluation is a labour-intensive process and brings a high risk of challenge. Our AI product is designed to streamline, automate, and enhance the scoring and review of tenders and supplier submissions for public sector organisations. The output is Procurement Act compliant tender evaluations. Key features include the automation of tender evaluation and scoring, secure document handling and audit trails, integration with procurement platforms and real-time analytics and reporting. Our service improves efficiency, reduces manual errors, and ensures compliance with the Procurement Act. It also provides transparency, auditability, and faster decision-making for public sector buyers.

Our service is hosted in UK-based, ISO 27001-certified Azure data centres, ensuring secure storage and processing. All data is encrypted in transit and at rest, with role-based access controls. Service levels include 99.9% availability during core business hours, proactive outage notifications, and scheduled maintenance communicated in advance. Support is available by phone and email Monday to Friday, 9am–5pm, with escalation paths for critical issues. Customisation options allow tailored scoring criteria and workflows. Ancillary services include training workshops, integration support, and resource augmentation for capacity challenges.

Customisation

Our service offers flexible configuration to meet organisational and project-specific needs. Users can customise the product to meet organisation policy and procedural requirements, including (a) policy on

failure of a mandatory requirements, (b) whether appendices are included in word counts, and (c) use of drawings and images in responses.

Customisation is carried out by Capita during deployment and can be adjusted later through configuration settings or by submitting a request to your dedicated Account Manager. Subject to Capita's approval, they will customise and/or reconfigure the product for the customer.

The benefit of this approach is that Capita will continue to assure their product meets those standards to which it has been certified.

Support Levels

The following support is included in our standard subscription cost:

- Deployment: dedicated support to ensure that clients access the solution effectively, including user training.
- In-life: ongoing support to ensure that the product continues to perform effectively, and also wider support to improve how the Procurement and wider business operate to maximise the value delivered by the product.

We also assign an Account Manager for each project, a single point of contact for any customer's queries. The Account Manager will oversee the project day-to-day and be responsible for all deliverables, as well as for any performance issues and escalations. Our Account Managers are available to support customers via phone or email Monday to Friday, 9 to 5 (UK time).

Service Levels

Our service will maintain 99.9% availability during core business hours, supported by resilient Azure infrastructure and proactive monitoring. Our Service Level Agreements (SLAs) include four different priority levels, from 'Low Impact' (Priority 4) to 'Critical Impact' (Priority 1). All priority levels have varying response and resolution times, as detailed in Section 4 (Service Scope).

Onboarding & Training

Customers will be supported through the following training options:

- Onsite training for hands-on support during deployment.
- Online training via interactive workshops and webinars.
- Self-service resources, including comprehensive user documentation, guides, and a searchable knowledge base.

Initially, we provide a secure portal for document upload and evaluation, with clear guidance on metadata requirements and compliance standards. The onboarding process includes tailored training sessions for evaluators, covering system navigation, scoring workflows, and audit trail interpretation. Comprehensive documentation and a knowledge base are available for self-service learning, complemented by interactive workshops for hands-on experience.

For technical assurance, we offer dedicated support channels, including priority case handling and escalation paths. Customers are expected to maintain current software updates and provide necessary diagnostic details for issue resolution, while we ensure GDPR-compliant data handling and secure remote access when required. Regular updates and feature enhancements are delivered through managed releases, with proactive communication on changes.

Our approach ensures customers can confidently leverage our service's capabilities to streamline procurement evaluations and maintain compliance with organisational and regulatory standards.

Security

Capita's security governance is built on internationally recognised standards and best practices. It operates an integrated framework aligned with ISO 27001, ensuring robust risk management and secure-by-design principles across all services. Policies mandate security throughout the software development

lifecycle, supported by regular audits, vulnerability assessments, and penetration testing. Governance includes clear roles, incident response procedures, and compliance with PCI DSS for regulated environments. We also follow guidance from the UK NCSC and NIST, embedding continuous improvement and accountability into its operations. This approach ensures confidentiality, integrity, and availability of data while meeting contractual and regulatory obligations.

Our service protects data at rest using AES-256 encryption across all storage layers, including Azure Blob Storage and Cosmos DB. Encryption keys are managed securely via Azure Key Vault with automated rotation and strict access controls. Data is logically and physically segregated by client, ensuring isolation within Capita's Azure tenant. Governance is enforced through Capita's Data Directives and retention policies, mandating quarterly archiving and removal of intermediate copies. Additional safeguards include role-based access control (RBAC), multi-factor authentication for administrative access, and compliance with ISO27001 standards. These measures ensure confidentiality, integrity and compliance, and apply to all stored data without exception.

Offboarding

When a customer stops using our service, we provide dedicated support with access and removal of data as part of the offboarding process, which prioritises secure data handling and service termination. For ease of access, customers can request a full export of both datasets through the secure portal or via an API endpoint at no extra cost. All customer data can be exported in open, portable formats (CSV, PDF/A) to ensure continuity. We then perform certified deletion of all data, including backups, in compliance with security and privacy standards.

Once the export is complete, data can be downloaded securely or transferred to another cloud environment of the customer's choice. This process maintains compliance with GDPR and organisational data governance policies. This is all done within 30 days of notification of contract end and the outlining of data extraction requirements.

Ancillary Services

A key add-on to our service is the deployment of resources to carry out the tender management activities to support customers with any capacity or capability challenges. We can also deliver training workshops, develop custom reports and provide integration support.

As a procurement consultancy and delivery partner for our customers, we also deliver a wide range of other ancillary procurement and commercial services. Our procurement and commercial experts specialise in the delivery of end-to-end public sector compliant procurements, opportunity assessments, business case development, category management, procurement and commercial strategy development, contract management, procurement analytics, savings delivery and procurement transformation.

2 Service Features

List factual capabilities of the service using bullet points. Avoid benefits or sales claims. You can use the same list of 10 given in the Service Level Response Document.

Our key service features are listed below:

1. Use AI to execute evaluation of tenders
2. Use AI to identify committed delivery beyond contract specification
3. Use AI to identify contract mobilisation obligations
4. Use AI to identify all contracted deliverables

3 Service Benefits

List the buyer-facing outcomes your service delivers. Each benefit should be supported by a corresponding feature. You can use the same list of 10 given in the Service Level Response Document.

Our key service benefits are listed below:

1. Improve speed and accuracy of evaluation of tenders
2. Reduce the risk of challenge to tender outcomes
3. Improve identification of delivery commitments
4. Improve identification of mobilisation obligations
5. Improve identification of contracted deliverables
6. Improve management of contracted deliverables

4 Service Scope

Explain what is included in the service subscription: functionality, hosting, updates, support, licence model. Make sure this is aligned to the pricing document.

Scoping Process

Before contract start we engage with users to describe our approach and answer any questions they may have. We also validate the suitability of our service against customers' requirement and help users finalise the scope of our service. We also ensure alignment of our service with our customers' specific requirements, including any required customisations – users can customise our product to meet organisation policy and procedural requirements, including (a) policy on failure of a mandatory requirements, (b) whether appendices are included in word counts, and (c) use of drawings and images in responses.

Hosting Options and Locations

UK-based, ISO 27001-certified data centres. Public cloud (Azure UK South/West) or private cloud options.

Service Levels

Our service will maintain 99.9% availability during core business hours, supported by resilient Azure infrastructure and proactive monitoring. The service is designed for high availability through redundant components, automated failover, and continuous health checks. Scheduled maintenance will be communicated in advance, and downtime will be minimised to protect critical procurement operations.

Service Level Agreements (SLAs):

- **Priority 1 (Critical Impact):** Full service outage affecting multiple users. Response: 15 minutes | Resolution: 4 business hours.
- **Priority 2 (High Impact):** Partial loss of service with no workaround. Response: 1 hour | Resolution: 8 business hours.
- **Priority 3 (Moderate Impact):** Service impairment with workaround available. Response: 4 hours | Resolution: 5 business days.
- **Priority 4 (Low Impact):** Minor issues not affecting normal service. Response: 4 hours | Resolution: 10 business days.

Escalation paths include Cloud Operations and senior management to ensure timely resolution. These SLAs align with Capita's enterprise standards for SaaS solutions.

Refunds: If availability falls below the guaranteed level, customers receive service credits as outlined in the CCS framework terms. These credits are applied to future invoices or refunded where applicable.

Outage Management

Our service is designed with robust monitoring and transparent communication to ensure service continuity. In the event of an outage, we follow a multi-channel reporting approach:

- **Public Dashboard:** Service status and incident updates are published on a secure web-based dashboard accessible to authorised users. This dashboard provides real-time visibility into system health, scheduled maintenance, and any ongoing disruptions.
- **API Access:** For organisations requiring automated monitoring, PRISM offers an API endpoint that exposes current service status and incident details in JSON format. This allows integration with client-side monitoring tools and supports proactive alerting within enterprise workflows.
- **Email Alerts:** Critical incidents trigger immediate email notifications to designated contacts. These alerts include a summary of the issue, estimated resolution time, and any recommended actions. For major outages, follow-up communications are issued at regular intervals until resolution.

Additionally, our service maintains a 99.9% availability SLA and implements continuous performance monitoring. Incident response is prioritised within one hour for critical issues, supported by a dedicated service team during UK business hours. This combination of real-time reporting, API integration, and direct communication ensures transparency and rapid response for all stakeholders.

Incident Management

Capita operates a structured incident management process aligned with ITIL and ISO 27001. Pre-defined workflows exist for common events such as service outages, security breaches, and data loss. Users report incidents via the central IT Service Management (ITSM) platform or Service Desk, providing details like impact, location, and error messages. Once logged, incidents are categorised, prioritised, and escalated as needed. Incident reports are generated through the ITSM tool, offering root cause analysis, resolution steps, and timelines. High-severity incidents trigger immediate response and post-incident reviews to ensure continuous improvement and compliance with contractual and regulatory obligations.

5 Disclaimer

Include compliance wording regarding confidentiality, versioning, and that all terms are subject to CCS Framework T&Cs.

The contents of this document are strictly confidential and may not be reproduced in whole or in part without the prior written consent of Capita. Please ensure that a similar obligation of confidentiality is placed upon any third parties. All products and services described in this response are subject to written confirmation and Capita's standard terms and conditions.

This document may contain references to products, concepts and plans that may or may not be included in the final commercial offer. The commercial offer, and any subsequent revisions of it, will describe those elements that will ultimately represent the final contractual commitment.