

**CONCLAVE IDAM SSO**

**CONTRACT REFERENCE: CCSO20A10**

**CONTRACT BETWEEN**

**CROWN COMMERCIAL SERVICE**

**&**

**BRICKENDON CONSULTING LIMITED**

**Digital Outcomes and Specialists 4 Framework Agreement**

**Call-Off Contract**

This Call-Off Contract for the Digital Outcomes and Specialists 4 Framework Agreement (RM1043.6) includes

[Part A - Order Form](#_heading=h.qbtyoq)

Part B – Terms and conditions

[1. Contract start date, length and methodology](#_heading=h.4d34og8)

[2. Supplier Staff](#_heading=h.2s8eyo1)

[3. Swap-out](#_heading=h.1ksv4uv)

[4. Staff vetting procedures](#_heading=h.2jxsxqh)

[5. Due diligence](#_heading=h.3j2qqm3)

[6. Warranties, representations and acceptance criteria](#_heading=h.1y810tw)

[7.](#_heading=h.1y810tw) [Business continuity and disaster recovery](#_heading=h.2xcytpi)

[8. \_Payment terms and VAT](#_heading=h.1ci93xb)

[9. Recovery of sums due and right of set-off](#_heading=h.147n2zr)

[10. Insurance](#_heading=h.23ckvvd)

[11. Confidentiality](#_heading=h.32hioqz)

[12. Conflict of Interest](#_heading=h.1v1yuxt)

[13. Intellectual Property Rights](#_heading=h.4f1mdlm)

[14. Data Protection and Disclosure](#_heading=h.28h4qwu)

[15. Buyer Data](#_heading=h.37m2jsg)

[16. Document and source code management repository](#_heading=h.3l18frh)

[17. Records and audit access](#_heading=h.206ipza)

[18. Freedom of Information (FOI) requests](#_heading=h.3ygebqi)

[19. Standards and quality](#_heading=h.2dlolyb)

[20. Security](#_heading=h.sqyw64)

[21. Incorporation of terms](#_heading=h.1jlao46)

[22. Managing disputes](#_heading=h.2iq8gzs)

[23. Termination](#_heading=h.xvir7l)

[24. Consequences of termination](#_heading=h.2w5ecyt)

[25. Supplier’s status](#_heading=h.1gf8i83)

[26. Notices](#_heading=h.2fk6b3p)

[27. Exit plan](#_heading=h.2szc72q)

[28. Staff Transfer](#_heading=h.279ka65)

[29. Help at retendering and handover to replacement supplier](#_heading=h.279ka65)

[30. Changes to Services](#_heading=h.36ei31r)

[31. Contract changes](#_heading=h.1ljsd9k)

[32. Force Majeure](#_heading=h.3jtnz0s)

[33. Entire agreement](#_heading=h.1d96cc0)

[34. Liability](#_heading=h.2pta16n)

[35. Waiver and cumulative remedies](#_heading=h.wnyagw)

[36. Fraud](#_heading=h.3gnlt4p)

[37. Prevention of bribery and corruption](#_heading=h.1vsw3ci)

[38. Legislative change](#_heading=h.2uxtw84)

[39. Publicity, branding, media and official enquiries](#_heading=h.1a346fx)

[40. Non Discrimination](#_heading=h.2981zbj)

[41. Premises](#_heading=h.38czs75)

[42. Equipment](#_heading=h.1nia2ey)

[43. Law and jurisdiction](#_heading=h.2mn7vak)

[44. Defined Terms](#_heading=h.3ls5o66)

[Part C - The Schedules](#_heading=h.qbtyoq)

[Schedule 1 - Requirements](#_heading=h.qbtyoq)

[Schedule 2 - Supplier’s response](#_heading=h.3abhhcj)

[Schedule 3 - Statement of Work (SOW), including pricing arrangements and Key Staff](#_heading=h.1pgrrkc)

[Schedule 4 - Contract Change Notice (CCN)](#_heading=h.49gfa85)

Schedule 5 - Balanced Scorecard

[Schedule 6 - Optional Buyer terms and conditions](#_heading=h.2olpkfy)

Schedule 7 - How Services are bought (Further Competition process)

Schedule 8 - Deed of guarantee

Schedule 9 - Processing, Personal Data and Data Subjects

Schedule 10 – Alternative Clauses

The Order Form (Part A), the Terms and Conditions (Part B), and the Schedules (Part C) will become the binding contract after the Further Competition Process has been concluded. Specific details will be added after the award of the Framework Agreement. The Order Form may include:

* Buyer and Supplier details
* contract term
* Deliverables
* location
* warranties
* staffing needs
* staff vetting procedure
* notice period for termination
* standards required (including security requirements)
* charges, invoicing method, payment methods and payment terms
* additional Buyer terms and conditions
* insurances
* business continuity and disaster recovery
* security
* governance
* methodology
* Buyer and Supplier responsibilities

During the lifetime of the Framework Agreement, the Call-Off Contract Order Form template will be regularly updated to ensure that it continues to meet user needs.

#

#

#

#

# Part A - Order Form

|  |  |
| --- | --- |
| **Buyer**  | Crown Commercial Service |
| **Supplier**  | Brickendon Consulting Limited |
| **Call-Off Contract Ref.** | CCSO20A10 |
| **Call-Off Contract title**  | Conclave IDAM SSO |
| **Call-Off Contract description**  | Crown Commercial Service requires a Single Sign On system to be developed, in order to provide a single point of entry to permit customer access to CCS procurement services. |
| **Call-Off Contract period**  | 25 weeks |
| **Start date**  | 3/11/2020 and is valid for 25 weeks. |
| **End date** | 26/04/2021 |
| **(Optional) Maximum Call-Off Contract Extension Period** | N/A |
| **Latest Extension Period End Date** | N/A |
| **Notice period (prior to the initial Call-Off Contract period) to trigger Call-Off Contract Extension** | 2 weeks |
| **Call-Off Contract value**  | £695,035.00 |
| **Charging method**  |

|  |  |
| --- | --- |
| Capped time and materials (CTM) |  |
| Price per story |  |
| Time and materials (T&M)  |  |
| Fixed price  | X |
| Other pricing method or a combination of pricing methods agreed by the Parties |  |

 |
| **Notice period for termination for convenience**  | 30 days |
| **Initial SOW package** | To be agreed within one week of contract award |

This Order Form is issued in accordance with the Digital Outcomes and Specialists Framework Agreement (RM1043.6).

|  |  |
| --- | --- |
| **Project reference:** | CCSO20A10 |
| **Buyer reference:** |  |
| **Order date:** | 3/11/2020  |
| **Purchase order:** | To be agreed within one week of contract award |
| **From:** | Crown Commercial ServiceREDACTED  |
| **To:** | Brickendon Consulting LimitedREDACTED  |
| **Together:** | the “Parties” |

**Principle contact details**

|  |  |  |
| --- | --- | --- |
| For the Buyer: | Name: | REDACTED  |
| Title: | REDACTED  |
| Email: | REDACTED  |
| Phone: | REDACTED  |
| For the supplier  | Name: | REDACTED  |
| Title: | REDACTED  |
| Email:  | REDACTED  |

**Data Protection Officers**

|  |  |  |
| --- | --- | --- |
| For the Buyer: | Name: | REDACTED  |
| Title: | REDACTED  |
| Email: | REDACTED  |
| Phone: | REDACTED  |
| For the supplier:  | Name: | REDACTED  |
| Title: | REDACTED  |
| Email: | REDACTED  |
| Phone: | REDACTED  |

|  |
| --- |
| **Buyer contractual requirements**  |
| **Digital outcomes and specialists services required:** | For the provision of a Single Sign On system to be developed in order to provide a single point of entry to permit customer access to CCS procurement services.  |
| **Warranty period** | 90 days from the date of Buyer acceptance of release. |
| **Location:** | REDACTED  |
| **Staff vetting procedures:** | The level of clearance for this requirement is: Security Clearance.  |
| **Standards:** | WCAG 2.1 AA standard to ensure CCS are compliant with Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018.Minimum Cyber Security Standard - <https://www.gov.uk/government/publications/the-minimum-cyber-security-standard>  |
| **Limit on supplier’s liability:** | As stated, in accordance to the Terms & Conditions. |
| **Insurance:** | As stated, in accordance to the Terms & Conditions. |
| **Supplier’s information** |
| **Commercially sensitive information:** | The Supplier’s response and price breakdown. |
| **Subcontractors / Partners:** | N/A |
| **Call-Off Contract Charges and payment**  |
| **The method of payment for the Call-Off Contract Charges** (GPC or BACS) | BACS |
| **Invoice details** | Invoices should have all details outlined within “Invoice information required” and sent to the location set out at “Who and where to send invoices to”.Payments can only be made following satisfactory delivery of pre-agreed certified products and deliverables.  |
| **Who and where to send invoices to:** | Invoices should be submitted to: REDACTED  |
| **Invoice information required –** eg PO, project ref, etc. | The Supplier should ensure that the invoice includes:1. Appropriate references to identify the services and contract which is being invoiced from;
2. A valid Purchase Order Number;
3. A breakdown of charges, including a separate line for VAT.
4. Payment will be made within 30 days following receipt of a correctly submitted invoice as detailed above.
 |
| **Invoice frequency** | Calendar Monthly |
| **Call-Off Contract value:** | £695,035.00 (excluding VAT) |

**Call-Off Contract Charges:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Task**  | **Details(Brief breakdown of what is involved in the Task)** | **Role** | **Daily Rate (£ GBP)** | **Anticipated Days** | **Total (£ GBP)** | **Total Task Cost (£ GBP)** |
| **Project Set up** | Governance Set up and initiate | Level 7 - Set strategy or inspire |  REDACTED  | REDACTED  | REDACTED  | REDACTED  |
| Design core system architecture | Level 7 - Set strategy or inspire | REDACTED  | REDACTED  | REDACTED  |
| Project Plan and sign off | Level 7 - Set strategy or inspire | REDACTED  | REDACTED  | REDACTED  |
| Resource plan and sign off | Level 6 - Initiate or influence | REDACTED  | REDACTED  | REDACTED  |
| Resource mobilisation | Level 6 - Initiate or influence | REDACTED  | REDACTED  | REDACTED  |
| **Authentication and IDV MVP** | Environment setup | Level 4 - Enable | REDACTED  | REDACTED  | REDACTED  | REDACTED  |
| Design core system architecture | Level 7 - Set strategy or inspire | REDACTED  | REDACTED  | REDACTED  |
| Development and Testing - IDV MVP | Level 5 - Ensure or advise | REDACTED  | REDACTED  | REDACTED  |
| Launch - IDV MVP | Level 4 - Enable | REDACTED  | REDACTED  | REDACTED  |
| **SSO MVP** | Environment setup | Level 4 - Enable | REDACTED  | REDACTED  | REDACTED  | REDACTED  |
| Design core system architecture | Level 7 - Set strategy or inspire | REDACTED  | REDACTED  | REDACTED  |
| Development and Testing - SSO MVP | Level 5 - Ensure or advise | REDACTED  | REDACTED  | REDACTED  |
| Launch - SSO MVP | Level 4 - Enable | REDACTED  | REDACTED  | REDACTED  |
| **Authorisation Layer MVP** | Environment setup | Level 4 - Enable | REDACTED  | REDACTED  | REDACTED  | REDACTED  |
| Design core system architecture | Level 7 - Set strategy or inspire | REDACTED  | REDACTED  | REDACTED  |
| Development and Testing - Authorisation Layer MVP | Level 5 - Ensure or advise | REDACTED  | REDACTED  | REDACTED  |
| Launch - Authorisation Layer MVP | level 4 - Enable | REDACTED  | REDACTED  | REDACTED  |
| **Integration and User Onboarding** | Plan integration with two platforms | Level 6 - Initiate or influence | REDACTED  | REDACTED  | REDACTED  | REDACTED  |
| Identify users who will involve in POC | Level 6 - Initiate or influence | REDACTED  | REDACTED  | REDACTED  |
| CCS Platforms build for integration | Level 5 - Ensure or advise | REDACTED  | REDACTED  | REDACTED  |
| Integrate to Platform 1 (Salesforce) | Level 5 - Ensure or advise | REDACTED  | REDACTED  | REDACTED  |
| Integrate to Platform 2 (Jaeger) | Level 4 - Enable | REDACTED  | REDACTED  | REDACTED  |
| Onboard users | Level 4 - Enable | REDACTED  | REDACTED  | REDACTED  |
| **Infrastructure and Build** | Infrastructure & architecture sign off | Level 6 - Initiate or influence | REDACTED  | REDACTED  | REDACTED  | REDACTED |
| Infrastructure Procurement | Level 4 - Enable | REDACTED  | REDACTED  | REDACTED  |
| Network readiness and Environment setup | Level 4 - Enable | REDACTED  | REDACTED  | REDACTED  |
| **Solutions Delivery** | UI and UX layer | Level 5 - Ensure or advise | REDACTED  | REDACTED  | REDACTED  | REDACTED |
| API Layer Build | Level 6 - Initiate or influence | REDACTED  | REDACTED  | REDACTED  |
| Auth layer Feature enhancements and extensibility design | Level 4 - Enable | REDACTED  | REDACTED  | REDACTED  |
| Additional security and Token Management | Level 5 - Ensure or advise | REDACTED  | REDACTED  | REDACTED  |
| Testing | Level 4 - Enable | REDACTED  | REDACTED  | REDACTED  |
| **Migration** | User, account and Policy migration | Level 6 - Initiate or influence | REDACTED  | REDACTED  | REDACTED  | REDACTED |
| Data stores point to new platform | Level 4 - Enable | REDACTED  | REDACTED  | REDACTED  |
| Platform migration | Level 4 - Enable | REDACTED  | REDACTED  | REDACTED  |
| **Total Cost for this Requirement (Excluding VAT)( £ GBP)** |  £695,035.00  |
| **Role (According to Service Manual)** | **Description** | **Daily Rate (£ GBP)** |
| **Product Manager** | Your product manager works with the delivery team to:• Makes sure your service fits in with your organisation’s priorities• Define what the future goal of the service is (often called the ‘product vision’ in agile project management)• Make sure your service will meet user needs• Make sure your service is accessible to everyone, including people who have a disability• Prioritise user stories for each work sprint• Comment on technical, content and design solutions• Accept user stories when complete | REDACTED  |
| **Level 1 - follow** | as per our rate card with G-cloud | REDACTED  |
| **Level 2 - Assist** | as per our rate card with G-cloud | REDACTED  |
| **Level 3 - Apply** | as per our rate card with G-cloud | REDACTED  |
| **Level 4 - Enable** | as per our rate card with G-cloud | REDACTED  |
| **Level 5 - Ensure or advise** | as per our rate card with G-cloud | REDACTED  |
| **Level 6 - Initiate or influence** | as per our rate card with G-cloud | REDACTED  |
| **Level 7 - Set strategy or inspire** | as per our rate card with G-cloud | REDACTED  |
| **Service Owner** | Your service owner must have the decision-making authority to deliver on all aspects of a project. They also:• Have overall responsibility for developing, operating and continually improving your service• Represent the service during service assessments• Make sure the necessary project and approval processes are followed• Identify and mitigate risks to your project• Encourage the maximum possible take-up of your digital service• Have responsibility for your service’s assisted digital support |  |
| **Delivery Manager** | Your delivery manager is responsible for:• Setting up the agile environment your team needs to build and iterate a user-centred service• Removing obstacles or ‘blockers’ to progress• Helping your service team become better at autonomously organising their own work• Making sure accessibility is factored into each feature or activity the team’s working on |  |
| **User Research** | Your user researcher helps your team learn about the people who will use your service. This will help you design and build a service that works well for all your users, including people with a disability and those who need support.On your team, they will:• Plan and carry out research using a range of methods• Involve the team in user research to help everyone develop a deep understanding of your users• Create clear findings that help your team continuously improve your service, based on data and evidence |  |
| **Content Designer** | A content designer is responsible for the content in your service. They contribute to service design by:• Developing content plans and strategies based on user needs• Writing clear, usable and accessible content in plain English• Reviewing content to make sure it’s accurate, relevant, accessible and written in line with GOV.UK style• Communicating the principles of content design to your service team and others across your organisation• Advocating for users of your service by challenging requests that don’t support their needs |  |
| **Designer** | Designers help your team create user-focused, accessible services and a consistent user experience.Depending on the type of service you’re building, you may need a team of designers with a range of different skills, for example interaction, content, service or graphic designers.  |  |
| **Developer** | You need developers on your team to:• Build accessible software with a focus on what users need from your service and how they’ll use it• Advise on the technical feasibility of designs• Write, adapt, maintain and support code• Continually improve the service with new tools and techniques• Solve technical problems |  |
| **Performance analyst** | Performance analysts help your team understand and improve your service’s performance by:•Collecting and presenting key performance data and analysis for your service•Working with your service owner to make sure their service meets the performance requirements set out in the Service Standard•Helping your service team understand user needs by providing quantitative and qualitative evidence from web analytics, financial data and user feedback |  |
| **Technical Architect** | Technical architects need to:•Work with delivery teams and third parties to decide on technical requirements and improvements for software development and web operation•Make sure that new and updated platforms, products, transactions and system architectures are robust, scalable, open and secure |  |
| **DevOps Engineer** | DevOps engineers help your service team by:•Running your production systems•Helping the development team build software that’s easy to use•Working with developers to optimise existing applications and design new ones•Encouraging everyone (developers, delivery managers, product managers) to think about how new applications will be run and maintained |  |
| **Business Analyst** | Business analysts work with the service owner or product manager to:•Define what skills a service will need and map where these can be found (eg from an external contractor)•Check there’s the budget to cover the proposed approach•Analyse how much money your project needs for its ongoing running costs•Analyse and map risks and propose solutions |  |
| **Quality Assurers and Testers** | The quality of any digital service is the responsibility of the entire team, and the final responsibility lies with the service owner.Employing specialist skills from outside of the service is a good way to make sure this is tested thoroughly. You may find this particularly helpful for penetration testing and quality assurance.A quality assurer can work on a short-term basis with your team to build quality into everything they do. They should leave your team capable of managing quality as part of their standard development and iteration of the service. |  |

|  |
| --- |
| **Additional Buyer terms** |

|  |  |
| --- | --- |
| **Warranties, representations and acceptance criteria**  | See Annex A – Brickendon Non-Disclosure Agreement.No other additional warranties and undertakings are required.  |
| **Supplemental requirements in addition to the call-off terms** | None |
| **Buyer specific amendments to/refinements of the Call-Off Contract terms** | Not Applicable |
| **Specific terms:** | Not Applicable |

|  |
| --- |
| **Formation of Contract**  |
| * 1. By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.
 |
| * 1. The Parties agree that they have read the Order Form (Part A), the Call-Off Contract terms and conditions (Part B), and the Schedules (Part C), and by signing below agree to be bound by this Call-Off Contract.
 |
| * 1. In accordance with the Further Competition procedure set out in Section 3 of the Framework Agreement, this Call-Off Contract will be formed when the Buyer acknowledges the receipt of the signed copy of the Order Form from the Supplier (the “call-off effective date”).
	2. The Call-Off Contract outlines the Deliverables of the agreement. The Order Form outlines any amendment of the terms and conditions set out in Part B. The terms and conditions of the Call-Off Contract Order Form will supersede those of the Call-Off Contract standard terms and conditions.
1. **Background to the agreement**

(A) The Supplier is a provider of digital outcomes and specialists services and undertook to provide such Services under the terms set out in Framework Agreement number RM1043.6 (the “Framework Agreement”). (B) The Buyer served an Order Form for Services to the Supplier on the Order Date stated in the Order Form.(C) The Parties intend that this Call-Off Contract will not itself oblige the Buyer to buy or the Supplier to supply the Services. Specific instructions and requirements will have contractual effect on the execution of an SOW. |

**SIGNED:**

|  |  |  |
| --- | --- | --- |
|  | **Supplier:** | **Buyer:** |
| Name: | REDACTED | REDACTED |
| Title: | CEO |  |
| Signature: | REDACTED | REDACTED |
| Date: | 10 November 2020 |  |

##

## Part B – Terms and conditions

# 1. Call-Off Contract start date, length and methodology

1.1 The Supplier will start providing the Services in accordance with the dates specified in any Statement of Work (SOW).

1.2 Completion dates for Deliverables will be set out in any SOW.

1.3 Unless the Call-Off Contract period has been either increased in accordance with Clause 1.4 or decreased in accordance with Clause 1.5 then the term of the Call-Off Contract will end when the first of these occurs:

* the Call-Off Contract period End Date listed in the Order Form is reached; or
* the final Deliverable, specified in the final SOW, is completed.

1.4 The Buyer can extend the term of the Call-Off Contract by amending the Call-Off Contract End Date where:

* an Extension Period was specified in the Order Form; and
* written notice was given to the Supplier before the expiry of the notice period set out in the Order Form. The notice must state that the Call-Off Contract term will be extended, and must specify the number of whole days of the extension.

After this, the term of the Call-Off Contract will end on the last day of the Extension Period listed in the notice (the “Extension Period End Date”).

1.5 If the Call-Off Contract is terminated early, either during the initial Call-Off Contract period, or during any Extension Period, the term of the Call-Off Contract will end on the termination date.

1.6 The Supplier will plan on using an agile process, starting with user needs. The methodology will be outlined in the SOW. Waterfall methodology will only be used in exceptional circumstances, and where it can be shown to best meet user needs. Projects may need a combination of both waterfall and agile methods, playing to their respective strengths.

# 2. Supplier Staff

2.1 The Supplier Staff will:

* fulfil all reasonable requests of the Buyer;
* apply all due skill, care and diligence to the provisions of the Services;
* be appropriately experienced, qualified and trained to supply the Services;
* respond to any enquiries about the Services as soon as reasonably possible; and
* complete any necessary vetting procedures specified by the Buyer.

2.2 The Supplier will ensure that Key Staff are assigned to provide the Services for their Working Days (agreed between Supplier and Buyer) and are not removed from the Services during the dates specified in the relevant SOW.

2.3 The Supplier will promptly replace any Key Staff that the Buyer considers unsatisfactory at no extra charge. The Supplier will promptly replace anyone who resigns with someone who is acceptable to the Buyer. If the Supplier cannot provide an acceptable replacement, the Buyer may terminate the Call-Off Contract subject to clause 23.

2.4 Supplier Staff will comply with Buyer requirements for the conduct of staff when on Buyer’s premises.

2.5 The Supplier will comply with the Buyer’s staff vetting procedures for all or part of the Supplier Staff.

2.6 The Supplier will, on request (and subject to any obligations under the Data Protection Legislation), provide a copy of the contract of employment or engagement (between the Supplier and the Supplier Staff) for every member of Supplier Staff made available to the Buyer.

#

# 3. Swap-out

3.1 Supplier Staff providing the Services may only be swapped out with the prior approval of the Buyer. For this approval, the Buyer will consider:

* the provisions of Clause 2.1; and
* their Statement of Requirements and the Supplier’s response.

#

# 4. Staff vetting procedures

4.1 All Supplier Staff will need to be cleared to the level determined by the Buyer prior to the commencement of work.

4.2 The Buyer may stipulate differing clearance levels for different roles during the Call-Off Contract period.

4.3 The Supplier will ensure that it complies with any additional staff vetting procedures requested by the Buyer.

#

# 5. Due diligence

5.1 Both Parties acknowledge that information will be needed to provide the Services throughout the term of the Call-Off Contract and not just during the Further Competition process. Both Parties agree to share such information freely.

5.2 Further to Clause 5.1, both Parties agree that when entering into a Call-Off Contract, they:

5.2.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party

5.2.2 are confident that they can fulfil their obligations according to the terms of the Call-Off Contract

5.2.3 have raised all due diligence questions before signing the Call-Off Contract

5.2.4 have entered into the Call-Off Contract relying on its own due diligence

# 6. Warranties, representations and acceptance criteria

#

6.1 The Supplier will use the best applicable and available techniques and standards and will perform the Call-Off Contract with all reasonable care, skill and diligence, and according to Good Industry Practice.

6.2 The Supplier warrants that all Supplier Staff assigned to the performance of the Services have the necessary qualifications, skills and experience for the proper performance of the Services.

6.3 The Supplier represents and undertakes to the Buyer that each Deliverable will meet the Buyer’s acceptance criteria, as defined in the Call-Off Contract Order Form.

6.4 The Supplier undertakes to maintain any interface and interoperability between third-party software or Services and software or Services developed by the Supplier.

6.5 The Supplier warrants that it has full capacity and authority and all necessary authorisations, consents, licences and permissions to perform the Call-Off Contract.

# 7. Business continuity and disaster recovery

7.1 If required by the Buyer, the Supplier will ensure a disaster recovery approach is captured in a clear disaster recovery plan. All Supplier Staff must also adhere to the Buyer’s business continuity and disaster recovery procedure as required in the delivery of the Services for this project.

# 8. Payment terms and VAT

8.1 The Buyer will pay the Supplier within 30 days of receipt of an Electronic Invoice subject to the provisions of Clauses 8.5 and 8.6 or a valid invoice submitted in accordance with the Call-Off Contract.

8.2 The Supplier will ensure that each invoice or Electronic Invoice contains the information specified by the Buyer in the Order Form.

8.3 The Call-Off Contract Charges are deemed to include all Charges for payment processing. All invoices and Electronic Invoices submitted to the Buyer for the Services shall be exclusive of any Management Charge.

8.4 All payments under the Call-Off Contract are inclusive of VAT.

8.5 The Buyer shall accept and process for payment an Electronic Invoice submitted for payment by the Supplier where the invoice is undisputed and where it complies with the standard on electronic invoicing.

8.6 For the purposes of Clause 8.5 an Electronic Invoice complies with the standard on electronic invoicing where it complies with the European standard and any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870.

# 9. Recovery of sums due and right of set-off

#

9.1 The Buyer may retain or set-off payment of any amount owed to it by the Supplier if notice and reasons are provided.

# 10. Insurance

The Supplier will maintain the insurances required by the Buyer including those set out in this Clause.

10.1 Subcontractors

10.1.1 The Supplier will ensure that, during the Call-Off Contract, Subcontractors hold third-party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £5,000,000.

10.2 Agents and professional consultants

10.2.1 The Supplier will also ensure that all agents and professional consultants involved in the supply of Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the termination or expiry date to the Call-Off Contract to which the insurance relates.

10.3 Additional or extended insurance

10.3.1 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing insurance policies procured under the Framework Agreement.

10.3.2 The Supplier will provide CCS and the Buyer, the following evidence that they have complied with Clause 10.3.1 above:

* a broker's verification of insurance; or
* receipts in respect of the insurance premium; or
* other satisfactory evidence of payment of the latest premiums due.

10.4 Supplier liabilities

10.4.1 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or the Call-Off Contract.

10.4.2 Without limiting the other provisions of the Call-Off Contract, the Supplier will:

* take all risk control measures relating to the Services as it would be reasonable to expect of a contractor acting in accordance with Good Industry Practice, including the investigation and reports of claims to insurers;
* promptly notify the insurers in writing of any relevant material fact under any insurances of which the Supplier is, or becomes, aware; and
* hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of placing cover representing any of the insurance to which it is a Party.

10.4.3 The Supplier will not do or omit to do anything, which would entitle any insurer to refuse to pay any claim under any of the insurances.

10.5 Indemnity to principals

10.5.1 Where specifically outlined in the Call-Off Contract, the Supplier will ensure that the third-party public and products liability policy will contain an ‘indemnity to principals’ clause under which the Buyer will be compensated for both of the following claims against the Buyer:

* death or bodily injury; and
* third-party Property damage arising from connection with the Services and for which the Supplier is legally liable.

10.6 Cancelled, suspended, terminated or unrenewed policies

10.6.1 The Supplier will notify CCS and any Buyers as soon as possible if the Supplier becomes aware that any of the insurance policies have been, or are due to be, cancelled, suspended, terminated or not renewed.

10.7 Premium, excess and deductible payments

10.7.1 Where any insurance requires payment of a premium, the Supplier will:

* be liable for the premium; and
* pay such premium promptly.

10.7.2 Where any insurance is subject to an excess or deductible below the Supplier will be liable for it. The Supplier will not be entitled to recover any sum paid for insurance excess or any deductible from CCS or the Buyer.

#

# 11. Confidentiality

11.1 Except where disclosure is clearly permitted by the Call-Off Contract, neither Party will disclose the other Party’s Confidential Information without the relevant Party’s prior written consent.

11.2 Disclosure of Confidential Information is permitted where information:

* must be disclosed to comply with legal obligations placed on the Party making the disclosure
* belongs to the Party making the disclosure (who is not under any obligation of confidentiality) before its disclosure by the information owner
* was obtained from a third party who is not under any obligation of confidentiality, before receiving it from the disclosing Party
* is, or becomes, public knowledge, other than by breach of this Clause or the Call-Off Contract
* is independently developed without access to the other Party’s Confidential Information
* is disclosed to obtain confidential legal professional advice.

11.3 The Buyer may disclose the Supplier’s Confidential Information:

* to any central government body on the basis that the information may only be further disclosed to central government bodies;
* to the UK Parliament, Scottish Parliament or Welsh or Northern Ireland Assemblies, including their committees;
* if the Buyer (acting reasonably) deems disclosure necessary or appropriate while carrying out its public functions;
* on a confidential basis to exercise its rights or comply with its obligations under the Call-Off Contract; or
* to a proposed transferee, assignee or novatee of, or successor in title to, the Buyer.

11.4 References to disclosure on a confidential basis will mean disclosure subject to a confidentiality agreement or arrangement containing the same terms as those placed on the Buyer under this Clause.

11.5 The Supplier may only disclose the Buyer’s Confidential Information to Supplier Staff who are directly involved in the provision of the Services and who need to know the information to provide the Services. The Supplier will ensure that its Supplier Staff will comply with these obligations.

11.6 Either Party may use techniques, ideas or knowledge gained during the Call-Off Contract unless the use of these things results in them disclosing the other Party’s Confidential Information where such disclosure is not permitted by the Framework Agreement, or is an infringement of Intellectual Property Rights.

11.7 Information about orders placed by a Buyer (including pricing information and the terms of any Call-Off Contract) may be published by CCS and may be shared with other Buyers. Where Confidential Information is shared with other Buyers, CCS will notify the recipient of the information that its contents are confidential.

# 12. Conflict of Interest

12.1 The Supplier will take all appropriate steps to ensure that Supplier Staff are not in a position where there is or may be an actual conflict between the financial or personal interests of the Supplier Staff and another Supplier where both are providing the Services to the Buyer under any Call-Off Contract in accordance with the Framework Agreement.

12.2 Any breach of this Clause will be deemed to be a Material Breach.

12.3 A conflict of interest may arise in situations including where a member of the Supplier Staff:

* is related to someone in another Supplier team who both form part of the same team performing the Services under the Framework Agreement;
* has a business interest in another Supplier who is part of the same team performing the Services under the Framework Agreement;
* is providing, or has provided, Services to the Buyer for the discovery phase; or
* has been provided with, or had access to, information which would give the Supplier or an affiliated company an unfair advantage in a Further Competition procedure.

12.4 Where the Supplier identifies a risk of a conflict or potential conflict, they will (before starting work under the Call-Off Contract, unless otherwise agreed with the Buyer) inform the Buyer of such conflicts of interest and how they plan to mitigate the risk. Details of such mitigation arrangements are to be sent to the Buyer as soon as possible. On receiving this notification, the Buyer will, at its sole discretion, notify the Supplier if the mitigation arrangements are acceptable or whether the risk or conflict remains a Material Breach.

# 13. Intellectual Property Rights

13.1 Unless otherwise specified in the Call-Off Contract:

* the Buyer will not have any right to the Intellectual Property Rights (IPRs) of the Supplier or its licensors, including the Supplier Background IPRs and any IPRs in the Supplier Software.
* the Buyer may publish any Deliverable that is software as open source.
* the Supplier will not, without prior written approval from the Buyer, include any Supplier Background IPR or third party IPR in any Deliverable in such a way to prevent its publication and failure to seek prior approval gives the Buyer the right to use all Deliverables.
* the Supplier assigns (by present assignment of future rights to take effect immediately on it coming into existence) to the Buyer with full guarantee (or shall procure assignment to the Buyer), title to and all rights and interest in the Project-Specific IPRs together with and including any documentation, source code and object code comprising the Project-Specific IPRs and all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Project-Specific IPRs.
* the Supplier will not have any right to the Intellectual Property Rights of the Buyer or its licensors, including:
	+ the Buyer Background IPRs;
	+ the Project-Specific IPRs;
	+ IPRs in the Buyer Data.

13.2 Where either Party acquires, by operation of Law, rights to IPRs that are inconsistent with the allocation of rights set out above, it will assign in writing such IPRs as it has acquired to the other Party.

13.3 Except where necessary for the performance of the Call-Off Contract (and only where the Buyer has given its prior approval), the Supplier will not use or disclose any of the Buyer Background IPRs, Buyer Data or the Project-Specific IPRs to or for the benefit of any third party.

13.4 The Supplier will not include any Supplier Background IPRs or third-party IPRs in any release or Deliverable that is to be assigned to the Buyer under the Call-Off Contract, without approval from the Buyer.

13.5 The Supplier will grant the Buyer (and any replacement Supplier) a perpetual, transferable, sub-licensable, non-exclusive, royalty-free licence to copy, modify, disclose and use the Supplier Background IPRs for any purpose connected with the receipt of the Services that is additional to the rights granted to the Buyer under the Call-Off Contract and to enable the Buyer:

* to receive the Services;
* to make use of the Services provided by the replacement Supplier; and
* to use any Deliverables

and where the Supplier is unable to provide such a licence it must meet the requirement by creating new Project-Specific IPR at no additional cost to the Buyer.

13.6 The Buyer grants the Supplier a non-exclusive, non-assignable, royalty-free licence to use the Buyer Background IPRs, the Buyer Data and the Project-Specific IPRs during the term of the Call-Off Contract for the sole purpose of enabling the Supplier to provide the Services.

13.7 The Buyer gives no warranty as to the suitability of any IPRs licensed to the Supplier hereunder. Any such licence:

* may include the right to grant sub-licences to Subcontractors engaged in providing any of the Services (or part thereof) provided that any such Subcontractor has entered into a confidentiality undertaking with the Supplier on the same terms as in clause 11 (Confidentiality) and that any such subcontracts will be non-transferable and personal to the relevant Subcontractor; and
* is granted solely to the extent necessary for the provision of the Services in accordance with the Call-Off Contract. The Supplier will ensure that the Subcontractors do not use the licensed materials for any other purpose.

13.8 The Supplier will ensure that no unlicensed software or open source software (other than the open source software specified by the Buyer) is interfaced with or embedded within any Buyer Software or Deliverable.

13.9 Before using any third-party IPRs related to the supply of the Services, the Supplier will submit to the Buyer for approval, all details of any third-party IPRs.

13.10 Where the Supplier is granted permission to use third-party IPRs in a request for approval, the Supplier will ensure that the owner of such third-party IPRs grants to the Buyer a licence on the terms informed to the Buyer in the request for approval.

13.11 If the third-party IPR is made available on terms equivalent to the Open Government Licence v3.0, the request for approval will be agreed and the Supplier will buy licences under these terms. If not, the Supplier shall notify the Buyer in writing giving details of what licence terms can be obtained and other alternatives and no third-party IPRs may be used without Buyer approval in writing.

13.12 The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all losses which it may incur at any time as a result of any claim (whether actual alleged asserted and/or substantiated and including third party claims) that the rights granted to the Buyer in accordance with the Call-Off Contract or the performance by the Supplier of the provision of the Services or the possession or use by the Buyer of the Services or Deliverables delivered by the Supplier, including the publication of any Deliverable that is software as open source, infringes or allegedly infringes a third party’s Intellectual Property Rights (an ‘IPR Claim’).

13.13 Clause 13.12 will not apply if the IPR Claim arises from:

* designs supplied by the Buyer;
* the use of data supplied by the Buyer which is not required to be verified by the Supplier under any provision of the Call-Off Contract; or
* other material provided by the Buyer necessary for the provision of the Services.

13.14 The indemnity given in Clause 13.12 will be uncapped.

13.15 The Buyer will notify the Supplier in writing of the IPR Claim made against the Buyer and the Buyer will not make any admissions which may be prejudicial to the defence or settlement of the IPR Claim. The Supplier will at its own expense conduct all negotiations and any litigation arising in connection with the IPR Claim provided always that the Supplier:

* consults the Buyer on all substantive issues which arise during the conduct of such litigation and negotiations;
* takes due and proper account of the interests of the Buyer;
* considers and defends the IPR Claim diligently using competent counsel and in such a way as not to bring the reputation of the Buyer into disrepute; and
* does not settle or compromise the IPR Claim without the prior approval of the Buyer (such decision not to be unreasonably withheld or delayed).

13.16 If an IPR Claim is made (or in the reasonable opinion of the Supplier is likely to be made) in connection with the Call-Off Contract, the Supplier will, at the Supplier’s own expense and subject to the prompt approval of the Buyer, use its best endeavours to:

* modify the relevant part of the Services or Deliverables without reducing their functionality or performance, or substitute Services or Deliverables of equivalent functionality or performance, to avoid the infringement or the alleged infringement, provided that there is no additional cost or burden to the Buyer;
* buy a licence to use and supply the Services or Deliverables, which are the subject of the alleged infringement, on terms which are acceptable to the Buyer; and
* promptly perform any responsibilities and obligations to do with the Call-Off Contract.

13.17 If an IPR Claim is made (or in the reasonable opinion of the Supplier is likely to be made) against the Supplier, the Supplier will immediately notify the Buyer in writing.

13.18 If the Supplier does not comply with provisions of this Clause within 20 Working Days of receipt of notification by the Supplier from the Buyer under clause 13.15 or receipt of the notification by the Buyer from the Supplier under clause 13.17 (as appropriate), the Buyer may terminate the Call-Off Contract for Material Breach and the Supplier will, on demand, refund the Buyer with all monies paid for the Service or Deliverable that is subject to the IPR Claim.

13.19 The Supplier will have no rights to use any of the Buyer’s names, logos or trademarks without the Buyer’s prior written approval.

13.20 The Supplier will, as an enduring obligation throughout the term of the Call-Off Contract where any software is used in the provision of the Services or information uploaded, interfaced or exchanged with the CCS or Buyer systems, use software and the most up-to-date antivirus definitions from an industry-accepted antivirus software vendor. It will use the software to check for, contain the spread of, and minimise the impact of Malicious Software (or as otherwise agreed between CCS or the Buyer, and the Supplier).

13.21 If Malicious Software is found, the Supplier will co-operate with the Buyer to reduce the effect of the Malicious Software. If Malicious Software causes loss of operational efficiency or loss or corruption of Buyer Data, the Supplier will use all reasonable endeavours to help the Buyer to mitigate any losses and restore the provision of the Services to the desired operating efficiency as soon as possible.

13.22 Any costs arising from the actions of the Buyer or Supplier taken in compliance with the provisions of the above clause, and clause 20.3, will be dealt with by the Buyer and the Supplier as follows:

* by the Supplier, where the Malicious Software originates from the Supplier Software or the Buyer Data while the Buyer Data was under the control of the Supplier, unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier.
* by the Buyer if the Malicious Software originates from the Buyer Software or the Buyer Data, while the Buyer Data was under the control of the Buyer.

13.23 All Deliverables that are software shall be created in a format, or able to be converted into a format, which is suitable for publication by the Buyer as open source software, unless otherwise agreed by the Buyer, and shall be based on open standards where applicable. The Supplier warrants that the Deliverables:

* are suitable for release as open source;
* have been developed using reasonable endeavours to ensure that their publication by the Buyer shall not cause any harm or damage to any party using them;
* do not contain any material which would bring the Buyer into disrepute;
* can be published as open source without breaching the rights of any third party; and
* do not contain any Malicious Software.

13.24 Where Deliverables that are software are written in a format that requires conversion before publication as open source software, the Supplier shall also provide the converted format to the Buyer unless the Buyer agrees in advance in writing that the converted format is not required.

13.25 Where the Buyer has authorised a Supplier request not to make an aspect of the Deliverable open source, the Supplier shall as soon as reasonably practicable provide written details of what will not be made open source and what impact that exclusion will have on the ability of the Buyer to use the Deliverable and Project Specific IPRs going forward as open source.

13.26 The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to this clause to:

* a Central Government Body; or
* to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer.

If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in this clause.

# 14. Data Protection and Disclosure

14.1 The Parties will comply with the Data Protection Legislation and agree that the Buyer is the Controller and the Supplier is the Processor. The only processing the Supplier is authorised to do is listed at Schedule 9 unless Law requires otherwise (in which case the Supplier will promptly notify the Buyer of any additional processing if permitted by Law).

14.2 The Supplier will provide all reasonable assistance to the Buyer to prepare any Data Protection Impact Assessment before commencing any processing (including provision of detailed information and assessments in relation to processing operations, risks and measures) and must notify the Buyer immediately if it considers that the Buyer’s instructions infringe the Data Protection Legislation.

14.3 The Supplier must have in place Protective Measures, which have been reviewed and approved by the Buyer as appropriate, to guard against a Data Loss Event, which take into account the nature of the data, the harm that might result, the state of technology and the cost of implementing the measures.

14.4 The Supplier will ensure that the Supplier Personnel only process Personal Data in accordance with this Call-Off Contract and take all reasonable steps to ensure the reliability and integrity of Supplier Personnel with access to Personal Data, including by ensuring they:

  i) are aware of and comply with the Supplier’s obligations under this Clause;

ii) are subject to appropriate confidentiality undertakings with the Supplier or relevant Subprocessor

iii) are informed of the confidential nature of the Personal Data and don’t publish, disclose or divulge it to any third party unless directed by the Buyer or in accordance with this Call-Off Contract

iv) are given training in the use, protection and handling of Personal Data

14.5 The Supplier will not transfer Personal Data outside of the European Economic Area unless the prior written consent of the Buyer has been obtained and the following conditions are met:

1. the Buyer or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Buyer;
2. the Data Subject has enforceable rights and effective legal remedies;
3. the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Buyer in meeting its obligations); and
4. the Supplier complies with any reasonable instructions notified to it in advance by the Buyer with respect to the processing of the Personal Data

14.6 The Supplier will delete or return the Buyer’s Personal Data (including copies) if requested in writing by the Buyer at the termination or expiry of this Call-Off Contract, unless required to retain the Personal Data by Law.

14.7 The Supplier will notify the Buyer immediately if it receives any communication from a third party relating to the Parties’ obligations under the Data Protection Legislation, or it becomes aware of a Data Loss Event, and will provide the Buyer with full and ongoing assistance in relation to each Party’s obligations under the Data Protection Legislation in accordance with any timescales reasonably required by the Buyer.

14.8 The Supplier will maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:

1. the Buyer determines that the processing is not occasional;

ii) the Buyer determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

1. the Buyer determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

14.9 Before allowing any Subprocessor to process any Personal Data related to this Call-Off Contract, the Supplier must obtain the prior written consent of the Buyer, and shall remain fully liable for the acts and omissions of any Subprocessor.

14.10 The Buyer may amend this Call-Off Contract on not less than 30 Working Days’ notice to the Supplier to ensure that it complies with any guidance issued by the Information Commissioner’s Office.

#

# 15. Buyer Data

15.1 The Supplier will not remove any proprietary notices relating to the Buyer Data.

15.2 The Supplier will not store or use Buyer Data except where necessary to fulfil its obligations.

15.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested and in the format specified by the Buyer.

15.4 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.

15.5 The Supplier will ensure that any system which holds any Buyer Data complies with the security requirements prescribed by the Buyer.

15.6 The Supplier will ensure that any system on which the Supplier holds any protectively marked Buyer Data will be accredited as specific to the Buyer and will comply with:

The principles in the Security Policy Framework at <https://www.gov.uk/government/publications/security-policy-framework>

Government Security Classification policy at <https://www.gov.uk/government/publications/government-security-classifications>

Guidance issued by the Centre for Protection of National Infrastructure on Risk Management at <https://www.cpni.gov.uk/content/adopt-risk-management-approach>

 and Protection of Sensitive Information and Assets at <https://www.cpni.gov.uk/protection-sensitive-information-and-assets>

Government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at <https://www.gov.uk/government/publications/technology-code-of-practice/technologycode-of-practice>

The security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at <https://www.ncsc.gov.uk/guidance/implementingcloud-security-principles>

15.7 Where the duration of the Call-Off Contract exceeds one year, the Supplier will review the accreditation status at least once a year to assess whether material changes have occurred which could alter the original accreditation decision in relation to Buyer Data. If any changes have occurred, the Supplier will re-submit such system for accreditation.

15.8 If at any time the Supplier suspects that the Buyer Data that the Supplier has held, used, or accessed has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will at its own cost comply with any remedial action proposed by the Buyer.

15.9 The Supplier will provide, at the request of CCS or the Buyer, any information relating to the Supplier’s compliance with its obligations under the Data Protection Legislation. The Supplier will also ensure that it does not knowingly or negligently fail to do something that places CCS or any Buyer in breach of its obligations of the Data Protection Legislation. This is an absolute obligation and is not qualified by any other provision of the Call-Off Contract.

15.10 The Supplier agrees to use the appropriate organisational, operational and technological processes and procedures to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

# 16. Document and source code management repository

16.1 The Supplier will comply with any reasonable instructions given by the Buyer as to where it will store documents and source code, both finished and in progress, during the term of the Call-Off Contract.

16.2 The Supplier will ensure that all items that are uploaded to any repository contain sufficient detail, code annotations and instructions so that a third-party developer with the relevant technical abilities within the applicable role would be able to understand how the item was created and how it works together with the other items in the repository within a reasonable timeframe.

# 17. Records and audit access

17.1 The Supplier will allow CCS (and CCS’s external auditor) to access its information and conduct audits of the Services provided under the Call-Off Contract and the provision of Management Information (subject to reasonable and appropriate confidentiality undertakings).

# 18. Freedom of Information (FOI) requests

18.1 The Supplier will transfer any Request for Information to the Buyer within 2 Working Days of receipt.

18.2 The Supplier will provide all necessary help reasonably requested by the Buyer to enable the Buyer to respond to the Request for Information within the time for compliance set out in section 10 of the Freedom of Information Act or Regulation 5 of the Environmental Information Regulations.

18.3 To the extent it is permissible and reasonably practical for it to do so, CCS will make reasonable efforts to notify the Supplier when it receives a relevant FoIA or EIR request so that the Supplier may make appropriate representations.

# 19. Standards and quality

19.1 The Supplier will comply with any standards in the Call-Off Contract and Section 4 (How Services will be delivered) of the Framework Agreement, and with Good Industry Practice.

# 20. Security

20.1 If requested to do so by the Buyer, the Supplier will, within 5 Working Days of the date of the Call-Off Contract, develop, obtain Buyer’s approval of, maintain and observe a Security Management Plan and an Information Security Management System (ISMS) which, after Buyer approval, will apply during the term of the Call-Off Contract. Both the ISMS and the Security Management Plan will comply with the security policy of the Buyer and protect all aspects of the Services, and all processes associated with the delivery of the Services.

20.2 The Supplier will use software and the most up-to-date antivirus definitions available from an industry accepted antivirus software vendor to minimise the impact of Malicious Software.

20.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Buyer Data, the Supplier will help the Buyer to mitigate any losses and will restore the Services to their desired operating efficiency as soon as possible.

20.4 The Supplier will immediately notify CCS of any breach of security in relation to CCS’s Confidential Information (and the Buyer in relation to any breach regarding Buyer Confidential Information). The Supplier will recover such CCS and Buyer Confidential Information however it may be recorded.

20.5 Any system development by the Supplier must also comply with the government’s ‘10 Steps to Cyber Security’ guidance, as amended from time to time and currently available at: <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security> and secure development principles at : <https://www.ncsc.gov.uk/collection/developers-collection>

20.6 The Buyer will specify any security requirements for this project in the Order Form.

# 21. Incorporation of terms

#

21.1 Upon the execution of a Statement of Work (SOW), the terms and conditions agreed in the SOW will be incorporated into the Call-Off Contract that the terms of the SOW are agreed under.

# 22. Managing disputes

22.1 When either Party notifies the other of a dispute, both Parties will attempt in good faith to negotiate a settlement as soon as possible.

22.2 Nothing in this prevents a Party from seeking any interim order restraining the other Party from doing any act or compelling the other Party to do any act.

22.3 If the dispute cannot be resolved, either Party will be entitled to refer it to mediation in accordance with the procedures below, unless:

* the Buyer considers that the dispute is not suitable for resolution by mediation;
* the Supplier does not agree to mediation.

22.4 The procedure for mediation is as follows:

* A neutral adviser or mediator will be chosen by agreement between the Parties. If the Parties cannot agree on a mediator within 10 Working Days after a request by one Party to the other, either Party will as soon as possible, apply to the mediation provider or to the Centre for Effective Dispute Resolution (CEDR) to appoint a mediator. This application to CEDR must take place within 12 Working Days from the date of the proposal to appoint a mediator, or within 3 Working Days of notice from the mediator to either Party that they are unable or unwilling to act.
* The Parties will meet with the mediator within 10 Working Days of the mediator’s appointment to agree a programme for the exchange of all relevant information and the structure for negotiations to be held. The Parties may at any stage seek help from the mediation provider specified in this clause to provide guidance on a suitable procedure.
* Unless otherwise agreed, all negotiations connected with the dispute and any settlement agreement relating to it will be conducted in confidence and without prejudice to the rights of the Parties in any future proceedings.
* If the Parties reach agreement on the resolution of the dispute, the agreement will be recorded in writing and will be binding on the Parties once it is signed by their duly authorised representatives.
* Failing agreement, either Party may invite the mediator to provide a non-binding but informative opinion in writing. Such an opinion will be provided without prejudice and will not be used in evidence in any proceedings relating to the Call-Off Contract without the prior written consent of both Parties.
* If the Parties fail to reach agreement in the structured negotiations within 60 Working Days of the mediator being appointed, or such longer period as may be agreed by the Parties, then any dispute or difference between them may be referred to the courts.

22.5 Either Party may request by written notice that the dispute is referred to expert determination if the dispute relates to:

* any technical aspect of the delivery of the digital services;
* the underlying technology; or
* is otherwise of a financial or technical nature.

22.6 An expert will be appointed by written agreement between the Parties, but if there’s a failure to agree within 10 Working Days, or if the person appointed is unable or unwilling to act, the expert will be appointed on the instructions of the President of the British Computer Society (or any other association that has replaced the British Computer Society).

22.7 The expert will act on the following basis:

* they will act as an expert and not as an arbitrator and will act fairly and impartially;
* the expert's determination will (in the absence of a material failure to follow the agreed procedures) be final and binding on the Parties;
* the expert will decide the procedure to be followed in the determination and will be requested to make their determination within 30 Working Days of their appointment or as soon as reasonably practicable and the Parties will help and provide the documentation that the expert needs for the determination;
* any amount payable by one Party to another as a result of the expert's determination will be due and payable within 20 Working Days of the expert's determination being notified to the Parties
* the process will be conducted in private and will be confidential;
* the expert will determine how and by whom the costs of the determination, including their fees and expenses, are to be paid.

22.8 Without prejudice to any other rights of the Buyer under the Call-Off Contract, the obligations of the Parties under the Call-Off Contract will not be suspended, ceased or delayed by the reference of a dispute submitted to mediation or expert determination and the Supplier and the Supplier Staff will comply fully with the Requirements of the Call-Off Contract at all times.

# 23. Termination

23.1 The Buyer will have the right to terminate the Call-Off Contract at any time by giving the notice to the Supplier specified in the Order Form, subject to clause 23.2 and 23.3 below. The Supplier’s obligation to provide the Services will end on the date set out in the Buyer’s notice.

23.2 The minimum notice period (expressed in Working Days) to be given by the Buyer to terminate under this Clause will be the number of whole days that represent 20% of the total duration of the current SOW to be performed under the Call-Off Contract, up to a maximum of 30 Working Days.

23.3 Partial days will be discounted in the calculation and the duration of the SOW will be calculated in full Working Days.

23.4 The Parties acknowledge and agree that:

* the Buyer’s right to terminate under this Clause is reasonable in view of the subject matter of the Call-Off Contract and the nature of the Service being provided.
* the Call-Off Contract Charges paid during the notice period given by the Buyer in accordance with this Clause are a reasonable form of compensation and are deemed to fully cover any avoidable costs or losses incurred by the Supplier which may arise either directly or indirectly as a result of the Buyer exercising the right to terminate under this Clause without cause.
* Subject to clause 34 (Liability), if the Buyer terminates the Call-Off Contract without cause, they will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate such Loss. If the Supplier holds insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of such Loss, with supporting evidence of unavoidable Losses incurred by the Supplier as a result of termination.

23.5 The Buyer will have the right to terminate the Call-Off Contract at any time with immediate effect by written notice to the Supplier if:

* the Supplier commits a Supplier Default and if the Supplier Default cannot, in the opinion of the Buyer, be remedied; or
* the Supplier commits any fraud.

23.6 Either Party may terminate the Call-Off Contract at any time with immediate effect by written notice to the other if:

* the other Party commits a Material Breach of any term of the Call-Off Contract (other than failure to pay any amounts due under the Call-Off Contract) and, if such breach is remediable, fails to remedy that breach within a period of 15 Working Days of being notified in writing to do so;
* an Insolvency Event of the other Party occurs, or the other Party ceases or threatens to cease to carry on the whole or any material part of its business
* a Force Majeure Event occurs for a period of more than 15 consecutive calendar days.

23.7 If a Supplier Insolvency Event occurs, the Buyer is entitled to terminate the Call-Off Contract.

# 24. Consequences of termination

24.1 If the Buyer contracts with another Supplier, the Supplier will comply with Clause 29.

24.2 The rights and obligations of the Parties in respect of the Call-Off Contract (including any executed SOWs) will automatically terminate upon the expiry or termination of the relevant Call-Off Contract, except those rights and obligations set out in clause 24.6.

24.3 At the end of the Call-Off Contract period (howsoever arising), the Supplier must:

* immediately return to the Buyer:
	+ all Buyer Data including all copies of Buyer Software and any other software licensed by the Buyer to the Supplier under the Call-Off Contract;
	+ any materials created by the Supplier under the Call-Off Contract where the IPRs are owned by the Buyer;
	+ any items that have been on-charged to the Buyer, such as consumables; and
	+ all equipment provided to the Supplier. This equipment must be handed back to the Buyer in good working order (allowance will be made for reasonable wear and tear).
* immediately upload any items that are or were due to be uploaded to the repository when the Call-Off Contract was terminated (as specified in Clause 27);
* cease to use the Buyer Data and, at the direction of the Buyer, provide the Buyer and the replacement Supplier with a complete and uncorrupted version of the Buyer Data in electronic form in the formats and on media agreed with the Buyer and the replacement Supplier;
* destroy all copies of the Buyer Data when they receive the Buyer’s written instructions to do so or 12 months after the date of expiry or termination (whichever is the earlier), and provide written confirmation to the Buyer that the data has been destroyed, except where the retention of Buyer Data is required by Law;
* vacate the Buyer premises;
* work with the Buyer on any work in progress and ensure an orderly transition of the Services to the replacement supplier;
* return any sums prepaid for Services which have not been delivered to the Buyer by the date of expiry or termination;
* provide all information requested by the Buyer on the provision of the Services so that:
	+ the Buyer is able to understand how the Services have been provided; and
	+ the Buyer and the replacement supplier can conduct due diligence.

24.4 Each Party will return all of the other Party’s Confidential Information. Each Party will confirm that it does not retain the other Party’s Confidential Information except where the information must be retained by the Party as a legal requirement or where the Call-Off Contract states otherwise.

24.5 All licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Services will be terminated at the end of the Call-Off Contract period (howsoever arising) without the need for the Buyer to serve notice except where the Call-Off Contract states otherwise.

24.6 Termination or expiry of the Call-Off Contract will not affect:

* any rights, remedies or obligations accrued under the Call-Off Contract prior to termination or expiration;
* the right of either Party to recover any amount outstanding at the time of such termination or expiry;
* the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses:
	+ 8 - Payment Terms and VAT
	+ 9 - Recovery of Sums Due and Right of Set-Off
	+ 11 - Confidentiality
	+ 12 - Conflict of Interest
	+ 13 - Intellectual Property Rights
	+ 24 - Consequences of Termination
	+ 28 - Staff Transfer
	+ 34 - Liability
	+ 35 - Waiver and cumulative remedies
* any other provision of the Framework Agreement or the Call-Off Contract which expressly or by implication is to be performed or observed notwithstanding termination or expiry will survive the termination or expiry of the Call-Off Contract.

# 25. Supplier’s status

25.1 The Supplier is an independent Contractor and no contract of employment or partnership is created between the Supplier and the Buyer. Neither Party is authorised to act in the name of, or on behalf of, the other Party.

# 26. Notices

26.1 Any notices sent must be in writing. For the purpose of this Clause, an email is accepted as being in writing.

26.2 The following table sets out the method by which notices may be served under the Call-Off Contract and the respective deemed time and proof of Service:

|  |  |  |
| --- | --- | --- |
| **Delivery type** | **Deemed delivery time** | **Proof of Service** |
| Email | 9am on the first Working Day after sending | Dispatched in a pdf form to the correct email address, initially REDACTED, without any error message |

26.3 The address and email address of each Party will be the address and email address in the Order Form.

# 27. Exit plan

27.1 The Buyer and the Supplier will agree an exit plan during the Call-Off Contract period to enable the Supplier Deliverables to be transferred to the Buyer ensuring that the Buyer has all the code and documentation required to support and continuously develop the Service with Buyer resource or any third party as the Buyer requires. The Supplier will update this plan whenever there are material changes to the Services. A Statement of Work may be agreed between the Buyer and the Supplier to specifically cover the exit plan.

# 28. Staff Transfer 28.1 The Parties agree that nothing in the Call-Off Contract or the provision of the Services is expected to give rise to a transfer of employment to which the Employment Regulations apply. 28.2 The Supplier will fully indemnify the Buyer against all Supplier Staff Liabilities which arise as a result of any claims brought against the Buyer due to any act or omission of the Supplier or any Supplier Staff.

# 28.3 The indemnity given in Clause 28.2 will be uncapped.

# 29. Help at retendering and handover to replacement supplier

29.1 When requested, the Supplier will (at its own expense where the Call-Off Contract has been terminated before end of term due to Supplier cause) help the Buyer to migrate the Services to a replacement Supplier in line with the exit plan (Clause 27) to ensure continuity of the Services. Such help may include Supplier demonstrations of the existing code and development documents, software licences used and Buyer approval documents. The Supplier will also answer Service and development-related clarification questions.

29.2 Within 10 Working Days of a request by the Buyer, the Supplier will provide any information needed by the Buyer to prepare for any procurement exercise or to facilitate any potential replacement Supplier undertaking due diligence. The exception to this is where such information is deemed to be Commercially Sensitive Information, in which case the Supplier will provide the information in a redacted form.

# 30. Changes to services

30.1 It is likely that there will be changes to the scope of the Services during the Call-Off Contract period. Agile projects have a scope that will change over time. The detailed scope (eg as defined in user stories) can evolve and change during the Call-Off Contract Period. These changes do not require formal contract changes but do require the Buyer and Supplier to agree these changes.

30.2 Any changes to the high-level scope of the Services must be agreed between the Buyer and Supplier. The Supplier will consider any request by the Buyer to change the scope of the Services, and may agree to such request.

# 31. Contract changes

31.1 All changes to the Call-Off Contract which cannot be accommodated informally as described in Clause 30 will require a Contract Change Note.

31.2 Either Party may request a contract change by completing and sending a draft Contract Change Note in the form in Schedule 4 of Part C - The Schedules ('the **Contract Change Notice'**) to the other Party giving sufficient information to enable the other Party to assess the extent of the change and any additional cost that may be incurred. The Party requesting the contract change will bear the costs of preparation of the Contract Change Notice. Neither Party will unreasonably withhold nor delay consent to the other Party’s proposed changes to the Call-Off Contract.

31.3 Due to the agile-based delivery methodology recommended by the Framework Agreement, it may not be possible to exactly define the consumption of Services over the duration of the Call-Off Contract in a static Order Form. The Supplier should state the initial value of all Services that are likely to be consumed under the Call-Off Contract.

# 32. Force Majeure

#

32.1 Neither Party will be liable to the other Party for any delay in performing, or failure to perform, its obligations under the Call-Off Contract (other than a payment of money) to the extent that such delay or failure is a result of a Force Majeure event. Each Party will use all reasonable endeavours to continue to perform its obligations under the Call-Off Contract for the length of a Force Majeure event. If a Force Majeure event prevents a Party from performing its obligations under the Call-Off Contract for more than 15 consecutive calendar days, the other Party may terminate the Call-Off Contract with immediate effect by notice in writing.

# 33. Entire agreement

33.1 The Call-Off Contract constitutes the entire agreement between the Parties relating to the matters dealt within it. It supersedes any previous agreement between the Parties relating to such matters.

33.2 Each of the Parties agrees that in entering into the Call-Off Contract it does not rely on, and will have no remedy relating to, any agreement, statement, representation, warranty, understanding or undertaking (whether negligently or innocently made) other than as described in the Call-Off Contract.

33.3 Nothing in this Clause or Clause 34 will exclude any liability for (or remedy relating to) fraudulent misrepresentation or fraud.

# 34. Liability

34.1 Neither Party excludes or limits its liability for:

* death or personal injury;
* bribery or fraud by it or its employees;
* breach of any obligation as to title implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Goods and Services Act 1982; or
* any liability to the extent it cannot be excluded or limited by Law.

34.2 In respect of the indemnities in Clause 13 (Intellectual Property Rights) and Clause 28 (Staff Transfer) and a breach of Clause 14 (Data Protection and Disclosure) the Supplier’s total liability will be unlimited. Buyers are not limited in the number of times they can call on this indemnity.

34.3 Subject to the above, each Party's total aggregate liability relating to all Losses due to a Default in connection with this agreement will be limited to the greater of the sum of £500,000 or a sum equal to 200% of the Call-Off Contract Charges paid, due or which would have been payable under the Call-Off Contract in the 6 months immediately preceding the event giving rise to the liability.

* Losses covered by this clause 34.3 that occur in the first 6 months of a Call-Off Contract, will be limited to the greater of the sum of £500,000 or a sum equal to 200% of the estimated Call-Off Contract Charges for the first 6 months of the Call-Off Contract.

34.4 Subject to clause 34.1, in no event will either Party be liable to the other for any:

* loss of profits;
* loss of business;
* loss of revenue;
* loss of or damage to goodwill;
* loss of savings (whether anticipated or otherwise); or
* any indirect, special or consequential loss or damage.

34.5 The Supplier will be liable for the following types of loss which will be regarded as direct and will be recoverable by the Buyer:

* the additional operational or administrative costs and expenses arising from any Material Breach; and/or
* any regulatory losses, fines, expenses or other losses arising from a breach by the Supplier of any Law.

34.6 No enquiry, inspection, approval, sanction, comment, consent, or decision at any time made or given by, or on behalf of, the Buyer to any document or information provided by the Supplier in its provision of the Services, and no failure of the Buyer to discern any defect in, or omission from, any such document or information will exclude or limit the obligation of the Supplier to carry out all the obligations of a professional Supplier employed in a client and Buyer relationship.

34.7 Unless otherwise expressly provided, the obligations of the Buyer under the Call-Off Contract are obligations of the Buyer in its capacity as a contracting counterparty and nothing in the Call-Off Contract will be an obligation on, or in any other way constrain the Buyer in any other capacity, nor will the exercise by the Buyer of its duties and powers in any other capacity lead to any liability under the Call-Off Contract on the part of the Buyer to the Supplier.

34.8 Any liabilities which are unlimited will not be taken into account for the purposes of establishing whether any limits relating to direct loss or damage to physical Property within this Clause have been reached.

34.9 Each Party must use all reasonable endeavours to mitigate any Loss or damage which it suffers under or in connection with this Call-Off Contract, including any indemnities.

# 35. Waiver and cumulative remedies

35.1 The rights and remedies provided by this agreement may be waived only in writing by the Buyer or the Supplier representatives in a way that expressly states that a waiver is intended, and such waiver will only be operative regarding the specific circumstances referred to.

35.2 Unless a right or remedy of the Buyer is expressed to be exclusive, the exercise of it by the Buyer is without prejudice to the Buyer’s other rights and remedies. Any failure to exercise, or any delay in exercising, a right or remedy by either Party will not constitute a waiver of that right or remedy, or of any other rights or remedies.

# 36. Fraud

36.1 The Supplier will notify the Buyer if it suspects that any fraud has occurred, or is likely to occur. The exception to this is if while complying with this, it would cause the Supplier or its employees to commit an offence.

36.2 If the Supplier commits any fraud relating to a Framework Agreement, the Call-Off Contract or any other Contract with the government:

* the Buyer may terminate the Call-Off Contract
* CCS may terminate the Framework Agreement
* CCS and/or the Buyer may recover in full from the Supplier whether under Clause 36.3 below or by any other remedy available in law.

36.3 The Supplier will, on demand, compensate CCS and/or the Buyer, in full, for any loss sustained by CCS and/or the Buyer at any time (whether such loss is incurred before or after the making of a demand following the indemnity hereunder) in consequence of any breach of this Clause.

# 37. Prevention of bribery and corruption

#

37.1 The Supplier will not commit any Prohibited Act.

37.2 The Buyer and CCS will be entitled to recover in full from the Supplier and the Supplier will, on demand, compensate CCS and/or the Buyer in full from and against:

* the amount of value of any such gift, consideration or commission; and
* any other loss sustained by CCS and/or the Buyer in consequence of any breach of this Clause

# 38. Legislative change

38.1 The Supplier will neither be relieved of its obligations under the Call-Off Contract nor be entitled to increase the Call-Off Contract prices as the result of a general change in Law or a Specific Change in Law without prior written approval from the Buyer.

# 39. Publicity, branding, media and official enquiries

39.1 The Supplier will take all reasonable steps to not do anything which may damage the public reputation of the Buyer. The Buyer may terminate the Call-Off Contract for Material Breach where the Supplier, by any act or omission, causes material adverse publicity relating to or affecting the Buyer or the Call-Off Contract. This is true whether or not the act or omission in question was done in connection with the performance by the Supplier of its obligations hereunder.

#

# 40. Non Discrimination

40.1 The Supplier will notify CCS and relevant Buyers immediately of any legal proceedings issued against it by any Supplier Staff on the grounds of discrimination.

#

# 41. Premises

41.1 Where either Party uses the other Party’s premises, such Party is liable for all Loss or damage it causes to the premises. Such Party is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

41.2 The Supplier will use the Buyer’s premises solely for the Call-Off Contract.

41.3 The Supplier will vacate the Buyer’s premises upon termination or expiry of the Call-Off Contract.

41.4 This Clause does not create any tenancy or exclusive right of occupation.

41.5 While on the Buyer’s premises, the Supplier will:

* ensure the security of the premises;
* comply with Buyer requirements for the conduct of personnel;
* comply with any health and safety measures implemented by the Buyer;
* comply with any instructions from the Buyer on any necessary associated safety measures; and
* notify the Buyer immediately in the event of any incident occurring on the premises where that incident causes any personal injury or damage to Property which could give rise to personal injury.

41.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

41.7 All Equipment brought onto the Buyer’s premises will be at the Supplier's risk. Upon termination or expiry of the Call-Off Contract, the Supplier will remove such Equipment.

# 42. Equipment

42.1 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

42.2 Upon termination or expiry of the Call-Off Contract, the Supplier will remove the Equipment, and any other materials, leaving the premises in a safe and clean condition.

#

# 43. Law and jurisdiction

43.1 The Call-Off Contract will be governed by the Laws of England and Wales. Each Party agrees to submit to the exclusive jurisdiction of the courts of England and Wales and for all disputes to be conducted within England and Wales.

#

# 44. Defined Terms

|  |  |
| --- | --- |
| **‘Assurance’** | The verification process undertaken by CCS as described in section 5 of the Framework Agreement |
| **‘Background IPRs’** | Any and all IPR that are owned by or licensed to either Party and which are or have been developed independently of the Call-Off Contract (whether prior to the start date or otherwise) |
| **‘Buyer’** | A UK public sector body, or Contracting Authority, as described in the OJEU Contract Notice, that can execute a competition and a Call-Off Contract within the Framework Agreement |
| **‘Buyer Background IPRs’** | Background IPRs of the Buyer |
| **'Buyer’s Confidential Information'** | All Buyer Data and any information that relates to the business, affairs, developments, trade secrets, know-how, personnel, and Suppliers of the Buyer, including all Intellectual Property Rights (IPRs), together with all information derived from any of the aboveAny other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential') |
| **'Buyer Data'** | Data that is owned or managed by the Buyer, including Personal Data gathered for user research, eg recordings of user research sessions and lists of user research participants |
| **'Buyer Software'** | Software owned by or licensed to the Buyer (other than under or pursuant to this Call-Off Contract), which is or will be used by the Supplier for the purposes of providing the Services |
| **'Call-Off Contract'** | The legally binding agreement (entered into following the provisions of the Framework Agreement) for the provision of Services made between a Buyer and the SupplierThis may include the key information summary, Order Form, requirements, Supplier’s response, Statement of Work (SOW), Contract Change Notice (CCN) and terms and conditions as set out in the Call-Off Contract Order Form |
| **'Charges'** | The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under the Call-Off Contract, as set out in the applicable SOW(s), in consideration of the full and proper performance by the Supplier of the Supplier’s obligations under the Call-Off Contract and the specific obligations in the applicable SOW |
| **'Commercially Sensitive Information'** | Information, which CCS has been notified about, (before the start date of the Framework Agreement) or the Buyer (before the Call-Off Contract start date) with full details of why the Information is deemed to be commercially sensitive |
| **‘Comparable Supply’** | The supply of services to another customer of the Supplier that are the same or similar to any of the Services |
| **‘Confidential Information’**  | Buyer's Confidential Information or the Supplier's Confidential Information, which may include (but is not limited to):* any information that relates to the business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above
* any other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential')
 |
| **'Contracting Authority'** | The Buyer and any other person as listed in the OJEU Contract Notice or Regulation 2 of the Public Contracts Regulations 2015, as amended from time to time, including CCS |
| **'Control'** | Control as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly |
| **‘Controller’** | Takes the meaning given in the Data Protection Legislation. |
| **'Crown'** | The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf |
| **‘Data Loss Event’** | Any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Call-Off Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Call-Off Contract, including any Personal Data Breach**.** |
| **‘Data Protection Impact Assessment’** | An assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data. |
| **‘Data Protection Legislation’** | All applicable Law about the processing of personal data and privacy (including the GDPR, LED and DPA 2018) and including if applicable legally binding guidance and codes of practice issued by the Information Commissioner. |
| **‘Data Protection Officer’** | Takes the meaning given in the Data Protection Legislation. |
| **‘Data Subject’** | Takes the meaning given in the Data Protection Legislation. |
| **'Default'** | * any breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term)
* any other default, act, omission, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff in connection with or in relation to the Framework Agreement or this Call-Off Contract

Unless otherwise specified in this Call-Off Contract the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer |
| **'Deliverable'** | A tangible work product, professional service, outcome or related material or item that is to be achieved or delivered to the Buyer by the Supplier as part of the Services as defined in the Order Form and all subsequent Statement of Work |
| **'Digital Marketplace'** | The government marketplace where Services will be bought [(https://www.digitalmarketplace.service.gov.uk/](https://www.digitalmarketplace.service.gov.uk/)) |
| **‘DPA 2018’** | Data Protection Act 2018. |
| **‘Employment Regulations’** | The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the European Council Directive 77/187/EEC on the approximation of laws of European member states relating to the safeguarding of employees’ rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses, as amended or re-enacted from time to time |
| **‘Electronic Invoice’** | An invoice which has been issued, transmitted and received in a structured electronic format which allows for its automatic and electronic processing  |
| **'Equipment'** | The Supplier’s hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under the Call-Off Contract |
| **‘Extension Period’** | The period (expressed in Working Days) that the initial Call-Off Contract term is extended by following notice given by the Buyer to the Supplier in accordance with Clause 1.4, such period not to exceed the number of whole days that represent 25% of the initial Call-Off Contract period.  |
| **'FoIA'** | The Freedom of Information Act 2000 and any subordinate legislation made under the Act occasionally together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation |
| **‘Force Majeure’** | Force Majeure means anything affecting either Party's performance of their obligations arising from any of the following: ● acts, events, omissions, happenings or non-happenings beyond the reasonable control of the affected Party● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare● acts of government, local government or Regulatory Bodies● fire, flood, any disaster and any failure or shortage of power or fuel● an industrial dispute affecting a third party for which a substitute third party is not reasonably availableThe following do not constitute a Force Majeure event:● any industrial dispute relating to the Supplier, its staff, or any other failure in the Supplier’s (or a Subcontractor's) supply chain● any event or occurrence which is attributable to the wilful act, neglect or failure to take reasonable precautions against the event or occurrence by the Party concerned |
| **'Framework Agreement'** | The Framework Agreement between CCS and the Supplier for the provision of the Services dated 01/10/2019 |
| **‘Fraud’** | The making of a false representation or failing to disclose relevant information, or the abuse of position, in order to make a financial gain or misappropriate assets |
| **'Further Competition'** | The Further Competition procedure as described in Section 3 (how Services will be bought) of the Framework Agreement. |
| **‘GDPR’** | The General Data Protection Regulation (Regulation (EU) 2016/679). |
| **'Good Industry Practice'** | Standards and procedures conforming to the Law and the application of skill, care and foresight which would be expected from a person or body who has previously been engaged in a similar type of undertaking under similar circumstances. The person or body must adhere to the technology code of practice (<https://www.gov.uk/service-manual/technology/code-of-practice.html>) and the government service design manual (<https://www.gov.uk/service-manual>) |
| **'Group'** | A company plus any subsidiary or holding company.'Holding company' and 'Subsidiary' are defined in section 1159 of the Companies Act 2006 |
| **‘Group of Economic Operators’** | A partnership or consortium not (yet) operating through a separate legal entity.  |
| **'Holding Company'** | As described in section 1159 and Schedule 6 of the Companies Act 2006 |
| **'Information'** | As described under section 84 of the Freedom of Information Act 2000, as amended from time to time |
| **'Insolvency Event'** | may be:* a voluntary arrangement
* a winding-up petition
* the appointment of a receiver or administrator
* an unresolved statutory demand
* a Schedule A1 moratorium
 |
| **'Intellectual Property Rights' or 'IPR'** | means:a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, service marks, logos, database rights, trade marks, rights in internet domain names and website addresses and other rights in trade or business names, design rights (whether registerable or otherwise), know-how, trade secrets and moral rights and other similar rights or obligations whether registerable or not;b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; andc) all other rights whether registerable or not having equivalent or similar effect in any country or jurisdiction (including but not limited to the United Kingdom) and the right to sue for passing off. |
| **‘Key Staff’** | Means the Supplier Staff named in the SOW as such |
| **'KPI Target'** | The acceptable performance level for a key performance indicator (KPI)  |
| **'Law'** | Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body |
| **‘LED'** | Law Enforcement Direction (Directive (EU) 2016/680). |
| **'Loss'** | All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and 'Losses' will be interpreted accordingly |
|  **‘Lot’** | A subdivision of the Services which are the subject of this procurement as described in the OJEU Contract Notice |
| **'Malicious Software'** | Any software program or code intended to destroy, or cause any undesired effects. It could be introduced wilfully, negligently or without the Supplier having knowledge of its existence. |
| **'Management Charge'** | The sum paid by the Supplier to CCS being an amount of 1.0% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or termination of any Call-Off Contract |
| **'Management Information'** | The Management Information (MI) specified in section 6 of the Framework Agreement |
| **‘Management Information (MI) Failure’** | If any of the below instances occur, CCS may treat this as an 'MI Failure':* there are omissions or errors in the Supplier’s submission
* the Supplier uses the wrong template
* the Supplier’s report is late
* the Supplier fails to submit a report
 |
| **'Material Breach’ (Framework Agreement)**  | A breach by the Supplier of the following Clauses in the Framework Agreement: * Subcontracting
* Non-Discrimination
* Conflicts of Interest and Ethical Walls
* Warranties and Representations
* Provision of Management Information
* Management Charge
* Prevention of Bribery and Corruption
* Safeguarding against Fraud
* Data
* Intellectual Property Rights and Indemnity
* Confidentiality
* Official Secrets Act
* Audit
* Assurance
 |
| **'Material Breach’ (Call-Off Contract)**  | A single serious breach of or persistent failure to perform as required in the Call-Off Contract  |
| **'OJEU Contract Notice'** | The advertisement for this procurement issued in the Official Journal of the European Union |
| **'Order Form'** | An order in the form set out in Part A of the Call-Off Contract for Digital Outcome and Specialist Services placed by a Buyer with the Supplier |
| **'Other Contracting Authorities'** | All Contracting Authorities, or Buyers, except CCS |
| **'Party'** | * for the purposes of the Framework Agreement; CCS or the Supplier
* for the purposes of the Call-Off Contract; the Supplier or the Buyer,

 and 'Parties' will be interpreted accordingly |
| **'Personal Data'** | Takes the meaning given in the Data Protection Legislation. |
| **‘Personal Data Breach’** | Takes the meaning given in the Data Protection Legislation. |
| **‘Processing’** | This has the meaning given to it under the Data Protection Legislation but, for the purposes of this Framework Agreement and Call-Off Contract, it will include both manual and automatic processing. ‘Process’ and ‘processed’ will be interpreted accordingly. |
| **‘Processor’** | Takes the meaning given in the Data Protection Legislation. |
| **'Prohibited Act'** | To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:* induce that person to perform improperly a relevant function or activity
* reward that person for improper performance of a relevant function or activity
* commit any offence:
	+ under the Bribery Act 2010
	+ under legislation creating offences concerning Fraud
	+ at common Law concerning Fraud
	+ committing or attempting or conspiring to commit Fraud
 |
| **‘Project-Specific IPRs**’ | * Intellectual Property Rights in items, including Deliverables, created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of the Call-Off Contract and updates and amendments of these items including (but not limited to) database schema; and/or
* Intellectual Property Rights arising as a result of the performance of the Supplier's obligations under the Call-Off Contract;

but not including the Supplier Background IPRs |
| **'Property'** | The property, other than real property and IPR, issued or made available to the Supplier by the Buyer in connection with a Call-Off Contract |
| **‘Protective Measures’** | Appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it. |
| **'Regulations'** | The Public Contracts Regulations 2015 (at <http://www.legislation.gov.uk/uksi/2015/102/contents/made>) and the Public Contracts (Scotland) Regulations 2012 (at <http://www.legislation.gov.uk/ssi/2012/88/made>), as amended from time to time |
| **'Regulatory Bodies'** | Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in the Framework Agreement or the Call-Off Contract |
| **‘Release’** | The Deliverable for a particular Statement of Work. Its delivery by the Supplier and its acceptance by the Buyer completes the Statement of Work. |
| **'Reporting Date'** | The seventh day of each month following the month to which the relevant MI relates. A different date may be chosen if agreed between the Parties |
| **'Request for Information'** | A request for information or an apparent request under the Code of Practice on Access to Government Information, FoIA or the Environmental Information Regulations |
| **'Self Audit Certificate'** | The certificate in the form as set out in Framework Agreement Schedule 1 - Self Audit Certificate, to be provided to CCS by the Supplier in accordance with Framework Agreement Clause 7.6. |
| **'Services'** | Digital outcomes, digital specialists, user research studios or user research participants to be provided by the Supplier under this Call-Off Contract |
| **'Specific Change in Law'** | A change in the Law that relates specifically to the business of CCS or the Buyer and which would not affect a Comparable Supply |
| **'Statement of Requirements'** | A statement issued by CCS or any Buyer detailing its Services requirements issued in the Call-Off Contract |
| **'Statement of Work' (SOW)** | The document outlining the agreed body of works to be undertaken as part of the Call-Off Contract between the Buyer and the Supplier. This may include (but is not limited to) the Statement of Requirements, the Deliverable(s), the completion dates, the charging method. Multiple SOWs can apply to one Call-Off Contract |
| **'Subcontractor'** | Each of the Supplier’s Subcontractors or any person engaged by the Supplier in connection with the provision of the digital services as may be permitted by Clause 9.18 of the Framework Agreement or the Call-Off Contract  |
| **‘Subprocessor’** | Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract. |
| **‘Supplier’** | The Supplier of Digital Outcomes and Specialists services who successfully bid for Call-Off Contracts as outlined in the Contract Notice within the Official Journal of the European Union (OJEU Notice). The identifying details of the Supplier to be bound by the terms of this Call-Off Contract are set out in the Order Form. |
| **‘Supplier Background IPRs’** | Background IPRs of the Supplier |
| **‘Supplier Software’** | Software which is proprietary to the Supplier and which is or will be used by the Supplier for the purposes of providing the Services |
| **'Supplier Staff'** | All persons employed by the Supplier including the Supplier's agents and consultants used in the performance of its obligations under the Framework Agreement or the Call-Off Contract |
| **‘Supplier Staff Liabilities** | Any claims, actions, proceedings, orders, demands, complaints, Losses and any awards or compensation reasonably incurred in connection with any claim or investigation related to employment |
| **'Working Day'** | Any day other than a Saturday, Sunday or public holiday in England and Wales, from 9am to 5pm unless otherwise agreed with the Buyer and the Supplier in the Call-Off Contract |
| **‘VAT’** | Value added tax in accordance with the provisions of the Value Added Tax Act 1994 |

# Part C - The Schedules

# Schedule 1 - Requirements

1. **PURPOSE**
	1. The Delivery Partner (DP) will design and build a Single Sign-on (SSo) solution for Crown Commercial Service (CCS). The solution will provide a Single Sign on (SSO) facility with automated Identification and Verification (ID & V) capability for both internal and external stakeholders. System IPR will belong to CCS and will be capable of being internally run and managed. The Identification and Access Management System (IDAM) which is part of the solution will be based on a vendor supplied product. For the initial build SSO solution will be using AWS Cognito but will be designed to be portable to any IDAM that may be chosen, subject to additional implementation effort. .
2. **BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT**
	1. At the current time CCS has no Single Sign On (SSO) or single point of entry to permit customers access to CCS procurement services. Dependant on customer need and usage there are over 23 points of entry to the CCS procurement world, each entry point requiring its own individual login identity and password. Current systems have no automated identification verification systems or federation capability.
	2. The lack of a SSO causes the CCS user experience to be very disjointed and limits access to and usability of CCS services providing poor customer experience and a non-existent customer journey.  This causes elements of CCS services to lack consistency and involve repetitive processes which are inefficient and time consuming. An IDAM providing a SSO with a federated automated identification verification service is needed to ease and enhance customer experience and capability.
	3. The CCS IDAM will simplify and ease access to CCS services. The final IDAM solution will include a self-service management and password reset facility, bulk upload facility. The system and any associated IPR rights shall remain the sole property of CCS. The IDAM will be built using OAuth and OIDC. Federation will support SAML (and all parallel market technologies) and will be capable of federation with all current and future identity service providers. The system will also be capable of supporting unlimited API’s.
3. **DEFINITIONS**

|  |  |
| --- | --- |
| **Expression or Acronym** | **Definition** |
| CCS | means Crown Commercial Service, the Contracting Authority, the Buyer |
| DSD | means Digital Services Directorate |
| IDAM | means Identity Access and Management system |
| MVP | means Minimal Viable Product |
| SSO  | means Single Sign On |
| ID&V | means Identification and Verification |
| OAuth | means [The OAuth 2.0 Authorization Framework](https://tools.ietf.org/html/rfc6749) |
| SAML | means [Security Assertion Markup Language V2.0](https://www.oasis-open.org/standards#samlv2.0) |
| OIDC | means [Open ID Connect](https://openid.net/connect/)  |
| IPR | means Intellectual Property Rights |
| WCAG2.1AA | means [W3C Web Content Accessibility Guidelines, Level AA Conformance](https://www.w3.org/TR/WCAG21/) |
| SteerCo  | means Steering Group  |
| IdP | means Identity Provider |
| MFA  | means Multi Factor Authentication  |

1. **SCOPE OF REQUIREMENT**

Project scope includes, but is not limited to the following items:

1. Development and implementation of a system to manage user accounts and sign-on for an unlimited number of CCS and wider Government systems (all current and future CCS systems, with additional consideration for wider government services). NOTE: The user accounts will be managed initially in AWS Cognito but might be switched to an alternative vendor or bespoke build solution
2. Support for modern authentication mechanisms, including OIDC, SAML, associated technologies.
3. Designed and implemented to be secure to industry best practice.
4. Self-service password reset capability (for internal IdP users).
5. Bulk data upload facility (for internal IdP users).
6. Unlimited API integration capability.
7. Performing user testing prior to final signoff and product release
8. Integration with Central Identity Index Service (CII) - central index to identify organisations using external registers and indexes
9. Microservices architecture as detailed below (section 6.1)
10. The system shall be capable of internationalisation. Specifically, all front end and public access elements of the system must at a minimum be available in both English and Welsh languages (in compliance with ‘Welsh Language (Wales) Measure 2011’).
11. **THE REQUIREMENT**
	1. **High-Level Requirements**

The solution will provide a strategic authorisation, authentication and user management platform for CCS. Crucially, it will operate modern authentication standards and utilise external authentication mechanisms where possible, such as Google Sign-In for Google accounts, AzureAD (Office 365 subscriptions), Facebook, LinkedIn and others. User permissions will be managed by the user’s organisations maintaining custom claims and mapping these to internal CCS roles.

The solution will be based around a microservices architecture, with the following services implemented to work in conjunction with each other and other relied-upon and relying services to produce a robust, secure and easy-to-use authentication and authorisation service for CCS and it’s customers:

* **Authentication and authorisation service**s - providing authorisation and authentication services for user-facing services
* A **Security Service** - providing ID and access token management for back-end applications and resource services.
* A **User Profile** service - providing user management services such as a cached user profile picture, accessibility preferences, etc.)
* An **Organisation Profile** service - providing organisation management services such as category codes, trading locations, service contact details, role/group mappings, etc.
* A **Contacts service** - providing contact details such as phone numbers, email addresses, postal addresses, web addresses).
* A **CCS Identity Provider Service** - providing user authentication services on the same basis as any other identity provider (e.g. [Google](https://developers.google.com/identity/protocols/OpenIDConnect), [Facebook Login](https://developers.facebook.com/docs/facebook-login/overview/)), including MFA capabilities.
* A **Roles & Permissions Service** - handling the configuration and mapping of roles and permissions to external claims configurations.

The solution will need to integrate with the **Central Identity Index Service** (CII), which will be the mechanism by which organisations sign up to do business with CCS. On sign-up, an organisation will be created in the CII, along with minimal organisation profiles and a ‘root’ user profile.

The logical model of the proposed architecture is shown below. Green boxes represent areas within scope for delivery, peach boxes represent areas where integration is required.



All services and platforms will run on either the GOV.UK PaaS or the CCS AWS instance, and will conform to CCS, GDS and NCSC architectural, security and usability guidance and standards.

* 1. **Detailed Requirements**

The table below describes most of the detailed requirements which the service overall will be expected to meet:

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Persona** | **Requirements** | **Applies to** |
| 6 | As a user with CCS Administrator role I should be able to | remove role(s) from a user in response to a complaint.  | IDAM |
| 7 | As a user with CCS Administrator role I should be able to | add administrator role to a user | IDAM |
| 9 | As a user with CCS Administrator role I should be able to | check roles allocated to a user | IDAM |
| 10 | As a user with CCS Administrator role I should be able to | add the Organisational Identity Provider (IdP) Administrator role to a user | IDAM |
| 11 | As a user with CCS Administrator role I should be able to | initiate the CCS IdP user password reset process | IDAM |
| 20 | The system should | validate user connection (Location, device type, Network IP) against security criteria | IDAM |
| 21 | The system should | validate user profile against risk based security criteria | IDAM |
| 22 | The system should | timeout users after an agreed time if they are inactive | IDAM |
| 27 | As a user with an Organisational Admin role I should be able to | add other members of the organisation to the administration role | IDAM |
| 34 | As a user with an Organisational Admin role I should be able to | manage business role(s) provided to a user (buyer/supplier) | IDAM |
| 40 | As a user I should be able to | SSO - authenticate once onto all CCS applications per device (additional devices require re-authentication) | IDAM |
| 41 | As a user I should be able to | authenticate with the CCS IDAM directly | IDAM |
| 42 | As a user I should be able to | authenticate via a number of predetermined OIDC authentication providers | IDAM |
| 43 | As a user I should be able to | authenticate via my company’s OIDC, SAML or other federated authentication provider | IDAM |
| 44 | As a user I should be able to | register with the CCS IDAM directly | IDAM |
| 45 | As a user I should be able to | register with the CCS IDAM via a number of predetermined OIDC authentication providers | IDAM |
| 46 | As a user I should be able to | register with CCS IDAM via my company’s OIDC, SAML or other federated authentication provider | IDAM |
| 47 | As a user I should be able to | swap organisation I am representing if I have permission for a given organisation | IDAM (Delegation) |
| 91 | As a user I should be able to | Self service password reset capability (for CCS IdP) | IDAM |
| 92 | As a user I should be able to | SSO using OIDC and SAML protocols | IDAM |
| 49 | As a user with an Organisational Identity Provider (IdP) Admin role I should be able to | configure mappings between CCS role to OIDC roles and SAML assertions | IDAM |
| 51 | As an authenticated user the system should | swap role I am fulfilling for an organisation if I have permission within that organisation | IDAM |
| 52 | As an authenticated user the system should | apply to represent an organisation (user can apply for more organisation) | IDAM (Delegation) |
| 53 | As an authenticated user the system should | apply for a specific role for an organisation I represent | IDAM (Delegation) |
| 57 | As an authenticated user the system should | authenticate using the previous session’s IdP by default | IDAM |
| 58 | As an authenticated user the system should | leverage authentication services provided by my chosen IdP (MFA) | IDAM |
| 59 | As an authenticated user the system should | allow me to change my IdP at any time | IDAM |
| 61 | As an authenticated user the system should | use an agreed selection of security authentication (MFA) to authenticate to CCS IdP directly (but not SMS 2FA). | IDAM |
| 62 | As an authenticated user the system should | access Conclave services (Authentication, Registration and Service Catalogue) through a home portal page | IDAM |
| 63 | As an authenticated user the system should | access Conclave services (Authentication, Registration and Service Catalogue) via links from any CCS platform | IDAM |
| 88 | As a third party application provider, I should be able to | use Conclave to authenticate my services provided on behalf of CCS | IDAM |

|  |  |  |  |
| --- | --- | --- | --- |
| 25 | The system should | store and transmit data encrypted and in line with government security and cybersecurity policies | All |
| 26 | The system should | be compliant with any legislation such as GDPR related to individual supplier and buyer information. | All |
| 93 | The system should  | allow for the creation of organisation admin accounts within the CCS IdP via an API called from the CII service | All |

|  |  |  |  |
| --- | --- | --- | --- |
| 8 | As a user with CCS Administrator role I should be able to | check when an organisation has no active admin | Org Profile |
| 28 | As a user with an Organisational Admin role I should be able to | validate users are members of my organisation | Org Profile |
| 29 | As a user with an Organisational Admin role I should be able to | remove users from my organisation | Org Profile |
| 32 | As a user with an Organisational Admin role I should be able to | transfer a user from one organisation to another (within an organisational hierarchy) | Org Profile |
| 36 | As a user with an Organisational Admin role I should be able to | define complex organisational hierarchies. | Org Profile |
| 37 | As a user with Organisational Admin role the system should | notify me when a user applies to represent my organisation unless my organisation is federated | Org Profile |
| 38 | As a user with Organisational Admin role the system should | notify me when a user applies to be a buyer for my organisation unless my organisation is federated | Org Profile |

|  |  |  |  |
| --- | --- | --- | --- |
| 31 | As a user with an Organisational Admin role I should be able to | update user details | User Profile |
| 33 | As a user with an Organisational Admin role I should be able to | create a new user by cloning an existing user | User Profile |
| 35 | As a user with an Organisational Admin role I should be able to | bulk user upload through CSV or equivalent data file | User Profile |
| 55 | As an authenticated user the system should | update my personal information (name, contact details, etc.) where these are not provided via OIDC claims | User Profile |
| 56 | As an authenticated user the system should | update any CCS-specific preferences (commercial agreements, marketing preferences, etc.) | User Profile |
| 65 | As an authenticated user the system should | provide presentation style information based upon settings in my user profile (e.g. large type) | User Profile |

1. **KEY MILESTONES AND DELIVERABLES**
	1. Key milestones and deliverables critical to the fulfilment of the Contract are detailed at para 7.2 below.
	2. The following Contract milestones/deliverables shall apply:

|  |  |  |
| --- | --- | --- |
| **Milestone/Deliverable** | **Description** | **Timeframe or Delivery Date** |
| **1** | **Provision of SSO Solution design** | **Within 3 weeks of Contract Award**  |
| **2** | **Provision of SSO MVP including full rules and authorisation layer. Also to include integration of 2 CCS systems (CCS Salesforce instance and CCS Jaeger instance)** | **Within 25 weeks of Contract Award**  |
| **3** | **MVP is able to integrate with and support all new areas of CCS business (frameworks and any new platforms).** | **Within 25 weeks of Contract Award**  |
| **4** | **To assist CCS with draft of SOR, / design and process to support procurement of DP to support IDAM industrialisation across.** | **To be available at week 16 of the MVP build phase**  |

* 1. **Testing.** The vendor must meet all the functional and non-functional Requirements or User Stories and meet GDS standards for Accessibility and Security, which are based on WCAG 2.1.
	2. The following test criteria/material will be required:
		1. Test Strategy should be produced that outlines the delivery model, testing types, and quality measures, any constraints and risks.
		2. Non-functional Requirements or User Stories (Agile) including Accessibility, Security, Performance,
		3. Maintainability, Scalability, Resilience and Operational, should be documented by CCS.
		4. A Regression test pack should be maintained and available for execution in further iterations or releases.
		5. Regression Tests should be repeatable (i.e. automated) and packaged for testing in future deployments – adding to an automated regression test suite
		6. Test Data should be representative of the CCS data model
	3. **Delivery Partner Defect Standards.** The Delivery partner must meet the following defect stands upon product delivery:
		1. Defects identified during testing should be logged and an audit trail kept of root cause analysis (RCA) and fix details.
		2. Defects should be categorised using CCS classifications as described in slides 6 & 7
		3. List of open defects should be included in the Test Completion Summary report
		4. No Severity 1,2,3 defects should remain open at the end of the vendor test stages without agreement from CCS.

**NB**: Defects Severity and Priority are as classified by the International Software Testing Qualifications Board (ISTQB) definition

* 1. **Quality Assurance measures.** CCS reserve the right to conduct QA checks throughout the delivery lifecycle should this be required or be deemed necessary. The following ‘Quality Assurance Measures’ are required to be provided by the Delivery Partner:
		1. Test Strategy or equivalent document made available to CCS for review against quality criteria and for information
		2. Test Scenarios and Scripts made available to CCS to review against quality criteria and test coverage
		3. Test Results and Test Evidence available to CCS.
		4. Test Progress against plan and defect metrics reported at regular intervals to CCS.
		5. Wireframes / screen mock-ups provided to CCS prior to development, regular ‘Show n Tells’ during the software development lifecycle (SDLC).
1. **MANAGEMENT INFORMATION/REPORTING**
	1. The Potential Provider shall adhere to Government Digital Service guidelines regarding accessibility to their source code, transparency of regular communication and agile working methods. The output of management information must integrate with CCS’ report MI system.
	2. The dedicated CCS Delivery Manager (DM) will manage the stakeholder relationship and reporting. The DM will facilitate CCS elements of the project to assist delivery. The DM must be included at all relevant standups and receive detailed weekly product briefings. The selected Delivery Partner will be required to formally present project progress to the monthly project SteerCo. The DM will also attend and manage as required all other regular meetings, in addition to have sight of and access to all relevant project RAID , governance and management documentation/material.
2. **CONTINUOUS IMPROVEMENT**
	1. The Potential Provider will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.
	2. The Potential Provider shall present any suggested enhanced ways working or work processes to the DM as they are identified and to the SteerCo as required.
	3. Changes to the way in which the Services are to be delivered must be brought to the Buyer’s attention and agreed prior to any changes being implemented.
	4. There will be an agreed process to identify and apply any change or enhancement identified/requested by CCS to enhance/amend project scope/ capability. Where possible change will be cost neutral however, total for any CCS initiated change will not exceed 15% of the full contract price.
3. **QUALITY**
	1. As a CCS project it is expected that quality will be of the highest standard. Product code will be effective to run and will as a minimum meet industry standard and best practice. The IDAM must be capable of enhancement and adaption and is to be built as a series of interrelated, loosely-coupled micro services which can be easily updated as the technology picture advances. They following are to be included as quality requirements:
* Security (Zero critical/high risk defects).
* Highest levels of confidentiality and integrity of data,
* Maintainability (code reuse, well-known libraries, infrastructure components, ease of change).
* Usability (UAT) and match to requirements, performance - volumetrics and response time (difficult to measure - but essentially doesn't need too many resources, esp in cloud).
* Code quality (checked with code validators for security holes and style).
* Documentation of design, operating systems and all functionality and supporting material required to maintain and provide future updates of the system.
* Ensure any citizen facing software provided meets, as a minimum, the Web Content Accessibility Guidelines (WCAG) 2.1, AA standard.
1. **PRICE**
	1. Pricing will be on a ‘fixed price’ basis. The final payment which will not be less than 35% of the total price, will be made once the SSO Solution MVP has been delivered, tested by both CCS and GDS and been proven as an agreed suitable product
2. **STAFF AND CUSTOMER SERVICE**
	1. The Potential Provider shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.
	2. The Potential Provider’s staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.
	3. The Potential Provider shall ensure that staff understand the Buyer’s vision and objectives and will provide excellent customer service to the Buyer throughout the duration of the Contract.
	4. The Potential provider will ensure that the DM has full daily contact with the providers delivery team and delivery lead.
3. **SERVICE LEVELS AND PERFORMANCE**
	1. **The Buyer will measure the quality of the Supplier’s delivery by:**
		1. The Potential Bidder will be required to achieve the following service levels and KPIs and against which the Supplier’s performance will be assessed.

|  |  |  |  |
| --- | --- | --- | --- |
| **KPI / SLA** | **Service Area** | **KPI/SLA description** | **Target** |
| 1 | Service Delivery (SD) | Start Point | 100%  |
| 2 | SD | Delivery of full design | 100% |
| 3 | SD | Full design sign off | 100% |
| 4 | SD | Delivery of support documentation / meetings / process to stage 2 procurement.  | 100% |
| 5 | SD | Delivery of MVP | 100% |
| 6 | SD | Project completion and bug-fixing support prior to live deployment | 85% |
| 7 | SD | Supplier Resources delivering Services for the Contract to the required standard and with the correct skill/experience to successfully deliver.Measures:Number of Resources swapped outNumber of issues in delivered work formally raised or identified in writing between the Buyer and the SupplierRegularity of Issues in delivered work formally raised or identified in writing between the supplier. | 100% |
| 8 | SD | Resources provided should enable the successful delivery of all Milestones, Statements of Work (SoW) and Tasks to a high quality and accepted Standard by the Buyer. | 85% of Milestones, SoW & Tasks delivered & accepted by the Buyer without error or issue. |
| 9 | SD | Resources provided should promote a collaborative working relationship in a transparent and positive manner across teams.Measures:Number of conduct problems identified and formally brought to the Suppliers attention by the Buyer.Severity of conduct problems identified and formally brought to the Suppliers attention by the Buyer. | 100% of Attendance at all required and agreed meetings. |

* 1. 35% of the total cost for the IDAM will be paid following delivery of an effective, competent service which meets customer need and which conforms with the stipulated SoR’s. Should the provided system not be delivered to specification within the agreed timescale an element/or all of the final payment will be retained as compensation in lieu of service.
1. **SECURITY AND CONFIDENTIALITY REQUIREMENTS**
	1. The successful Supplier should obtain SC clearance prior to the services commencing.
	2. A Non-Disclosure Agreement will need to be signed before the Contract Award.
	3. Supplier should demonstrate that it operates a certified Information Security Management System (ISMS) programme. This should be supported by adequate security policies and security industry certifications (such as ISO27001, SOC2, Cyber Essentials Plus or equivalent) and must include the service procured in the certification scope
	4. Supplier must confirm and demonstrate that it conducts an independent penetration test or IT Health Check of its infrastructure and service regularly (ideally annually) and implements appropriate mitigation for all critical or high issues. Proof of this must be made available to the Authority on request
	5. The supplier must confirm and demonstrate that it has vulnerability and patch management processes in place
	6. The supplier must confirm and demonstrate adequate data handling controls for the lifecycle of any CCS data. This should include secure storage, processing, sharing and secure destruction controls
	7. The supplier must implement adequate encryption at rest and in transit for all data considered highly sensitive (e.g. personally identifiable information (PII), cardholder data, commercially sensitive). (e.g. AES256 at rest and TLS1.2 in transit)
	8. The supplier must demonstrate that it has a robust incident response plan and supporting processes in place to detect, respond, contain and recover from security breaches to the service
	9. The supplier must implement protective monitoring and maintain useful security logs (e.g. login, administrator actions) and have a mechanism in place to provide details of such logs upon Authority’s request (e.g. during security investigations, )
	10. The supplier shall take responsibility for ensuring that its suppliers supporting this delivery or service maintain a comparable level of security as per these requirements
2. **payment AND INVOICING**
	1. Payment for delivery of this product is on a fixed price basis. Payment will be made on a monthly basis with 65% of total payment will be divided equally over the time frame of the project a paid on a month by month basis with the final 35% of the invoice price being paid on successfully product delivery and testing of the product.

|  |  |
| --- | --- |
| Invoice Amount | Invoice Amount |
| 30 November 2020 | REDACTED  |
| 31 December 2020 | REDACTED  |
| 31 January 2021 | REDACTED  |
| 28 February 2021 | REDACTED  |
| 31 March 2021 | REDACTED  |
| On project completion in line with Clause 9.1 and subject to clauses 14.2-14.11 | REDACTED  |
| TOTAL | £695.035.00 + VAT |

* 1. A retained sum of 35% of the total Fixed price for the Contract will be kept in line with Clause 9.1
	2. At the end of the delivery period the solution will be reviewed and assessed by CCS or an agent on behalf of CCS. If the developed solution is delivered on time; meets the needs of CCS as per the scope of the Contract to an agreed accepted standard and free of critical and/or major defects then the retained sum of 35% will be payed in full. In the event of the final solution is not rejected by CCS it will be deemed accepted after 28 days.
	3. In the event of the final solution not being delivered on time and to a standard through no fault of CCS then the Supplier will have to continue work until the solution meets the scope to an agreed accepted standard, free from critical and/or major defects.
	4. The following deductions from the retained sum of 35% will occur if the solution is not delivered in line with the above on time (the Supplier will not be penalised for any delays caused by CCS):
		1. 0 - 7 Days late, no deduction
		2. 8-21 days late, 7.5% deduction, 27.5% paid.
		3. 22-30 Days Late, 15% deduction, 20% paid.
		4. 31-45 days Late, 20% deduction, 15% paid.
		5. 46+ days late, 25% deduction, 10% paid. CCS will also reserve the rights to terminate in line with Clause 23.6 and may seek to recover any losses in line with Clause 34.5
	5. Payments can only be made following satisfactory delivery of pre-agreed certified products and deliverables.
	6. Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.
	7. Work will be defined by Statements of Work under the call off.
	8. Invoices will be submitted monthly in arrears. The Buyer will pay the supplier within 30 days of receipt of the invoice.
	9. Invoices should be submitted to: REDACTED.
	10. Prices are to be submitted via the e-Sourcing Suite Attachment 4 – Price Schedule excluding VAT and including all other expenses relating to Contract delivery.
1. **CONTRACT MANAGEMENT**
	1. An initial meeting between the Buyer and Successful Supplier will take place at either the Buyer’s offices in London or the Suppliers offices within one week of contract commencement.
	2. Attendance at Contract Review meetings shall be at the Supplier’s own expense.

# Schedule 2 - Supplier’s response

We understand the challenges to integrate to the two identified systems, Salesforce and Jaeger, and also how to scale across the entire IT estate of more than 23 CCS points of entry. The user needs we detailed in the Conclave Discovery Phase was for the final IDAM solution to include a self-service management and password reset facility, plus a bulk upload facility. Because we understand the unique requirements of CCS and could see that no vendor product could satisfy these needs, we recommended not to purchase a vendor product but to build a system where CCS would be the sole owner including any associated IPR rights. Our solution includes SSO built using OAuth and OIDC. It will support SAML (and all parallel market technologies) and will be capable of federation with all current and future identity service providers. The system will also be capable of supporting unlimited APIs. The build investment will have 2-year ROI with approximately £240,000 annualised savings.

We know that fourteen (14) of the systems already support some form of Single Sign On (SSO) via AWS SSO and SRS SSO. Other systems have Individual Sign On (ISO). Of the systems with SSO not all enable all users access via SSO. Our understanding of the entire target architecture beyond this project enables us to ensure that our build is scalable to meet these User Needs. We also built strong relationships and a deep understanding of platforms that were applicable to all users (Buyers, Suppliers and CCS), those that were applicable to CCS and Buyers only, and those that were applicable to CCS and Suppliers only.

**Deliverables:**

* Sign-on for an unlimited number of User Accounts: CCS and wider Government systems: Brickendon designed the future state solution with CCS in the Discovery Phase. It is built on microservices architecture and fully scalable for SSO and an unlimited number of users. It will also enable wider government services to connect and utilise Multifactor Authentication (MFA) for approved platforms and services.
* Support for modern authentication mechanisms, Inl. OIDC, SAML, associated technologies. Brickendon’s solution for CCS includes adherence to SSO authentication using OIDC and SAML protocols. During Q1 2020 we delivered a SSO authentication layer for a client allowing authentication via Google, AWS, Azure, Facebook etc. We also recommended that 2FA should be considered as an extra authentication layer in the future state though not currently part of the requirements of this project.
* Designed and implemented to be secure to industry best practice: Brickendon’s solution is secure by design and to best practice including NCSC principles. The data classification for this project is “OFFICIAL” and our designed architecture ensures the data is compliant with relevant legislation like GDPR. See answers in 4.3 for our security in detail.
* Self-service password reset capability (for internal IdP users): Brickendon has designed and built self-service password reset capabilities on many other projects.
* Bulk data upload facility (for internal IdP users): Brickendon has designed and built permission based bulk data upload facilities on many other projects.
* Unlimited API integration capability: Brickendon’s solution for CCS is fully scalable for SSO and for an unlimited number of APIs. These will be built in accordance with the government approved API and data standards as detailed here: <https://www.gov.uk/guidance/gds-api-technical-and-data-standards>
* Performing user testing prior to final signoff and product release: Brickendon have an award-winning testing practice and will implement best practice methodologies to ensure testing is successfully conducted in all phases of the project including robust user testing prior to sign off and production release.
* Integration with Central Identity Index Service (CII) central index to identify: Brickendon’s solution will Integrate with CII for organisation identification using external registers and indexes. IDAM and eventually the Evidence Locker, via a RESTful API once development is finalised, will enable this data to be consumed by various services.
* Organisations using external registers and indexes: Brickendon’s solution enables organisations who use external registers and indexes to connect with the Conclave using Multifactor Authentication (MFA) or external services like AWS, Azure, Google, FB etc
* Microservices architecture (section 6.1): Brickendon build all our client developments on microservices architecture. This has many benefits for CCS. The code will easily scale and be readily reusable. It will enable better integration with third-party services and enable CCS to become fully DevOps with full automation as the need to test a monolithic code base is removed. This enables Conclave to deliver ‘faster, smaller, safer’ releases. This will also future proof the code base to enables certain services to change as required.
* Languages. Must be available at a minimum in English and Welsh languages: Brickendon’s Conclave SSO implementation will be fully compliant with multiple languages including the Welsh languages (in compliance with ‘Welsh Language (Wales) Measure 2011’)

# Understanding of CCS and proactive mitigation of Issues

During the Conclave Discover Phase, Brickendon found the current state analysis and requirements development took longer than planned due to slower than expected response from stakeholders. **We mitigated this issue** by firstly building a solid engagement framework with the stakeholders. We developed stakeholder relationships and a questionnaire to capture buyer and supplier input, conducted interviews of research groups to leverage previously performed research, and made frequent site visits to CCS and NQC offices in London, Liverpool and Manchester. F

# 1.1.2 Brickendon were proactive during the Conclave Discovery Phase

Brickendon didn’t just stop at assessing the current state of the existing platforms during the discovery phase. **We proactively looked for gaps both in functionality and in ability** to deliver a solution to meet the needs that CCS users required. This led to a deep understanding of which platforms should be targeted, and when, for integration into the future state. This understanding is beyond the current scope of this engagement. Finally, we proactively held review workshop to encourage all key stakeholders to participate in the requirements and formal signoffs.

Examples of proactivity during Conclave Discovery Phase;

* **Brickendon identified design and security gaps in SRS:** We proactively questioned SRS suitability for the future state solution. These specific issues were raised with CCS management who agreed this matter requires further investigation in the next phases of the project if SRS is to be part of the future state solution.
* **Brickendon identified challenges with the ID Federation to corporate directory:** It required agreement and cooperation by the buyer/supplier organisation. Brickendon highlighted that simple and clear guidelines for buyers and suppliers to explain the benefits of federation from their perspective, and an onboarding tutorial to answer potential questions are likely to increase the adoption rate. It is worth noting that Brickendon held similar roadshows at the other clients such as Credit Suisse, where of the target platform increased exponentially.
* **Brickendon identified that there might be challenges with existing vendors:** Cooperation with existing vendors following the communication of future roadmap might lead to challenges as the future state will undoubtedly be unfavourable for some. Brickendon believe addressing any procurement issues and securing assurances from vendors for their cooperation on supporting future roadmap will lead to a smoother transition for CCS.

1.1.3 Brickendon Programme Governance Framework Model:

Brickendon have a formal governance framework to ensure that the milestones of the project are met on time, or preferably ahead of time. We have reviewed the specific milestones of this engagement, as detailed in the table below, and believe our Programme Governance Framework is perfectly suited to deliver this programme on or ahead of schedule. We have already done work on the below milestones and see in [red] when we believe we can deliver these items for CCS

|  |  |  |
| --- | --- | --- |
| Milestone/ Deliverable  | Description  | Timeframe or Delivery Date  |
| 1  | Provision of SSO design  | Within 3 weeks of Contract Award \*\* on or ahead of schedule  |
| 2  | Provision of SSO MVP including full rules and authorisation layer. Also, to include integration of 2 CCS systems (CCS Salesforce instance and CCS Jaeger instance)  | Within 25 weeks of Contract Award \*\* on or ahead of schedule  |
| 3  | MVP is able to integrate with and support all new areas of CCS business (frameworks and any new platforms).  | Within 25 weeks of Contract Award \*\* on or ahead of schedule  |
| 4  | To assist CCS with draft of SOR, / design and process to support procurement of DP to support IDAM industrialisation across.  | To be available at week 16 of the MVP build phase \*\* on or ahead of schedule  |

Our Programme Governance Framework is perfectly suited to deliver the milestones of this programme as detailed above.



The above diagram shows the high-level framework. Below we detail further items under each of the categories above:

* **Governance:** Framework and structure processes put in place to deliver outcomes and outputs. Includes all aspects of programme and project planning, capacity planning, quality management and test plans, budgeting, defining roles and responsibilities across the project and wider stakeholder group, completion of the terms of engagement, terms of reference (ToR), and resource skills matrix.
* **Operations:** Programme reporting including milestone reporting to plan, status reporting, financial reporting, risk and issue reporting and all other management reports as to effectively manage the deliverables. This includes managing the change control process encompassing change delivery, change management, business impact analysis, quality control, resource and programme finance tracking to plan.
* **Tools:** project management, milestone tracking systems (ie JIRA), source repository systems (ie Github) and all others required to perform activities or store artefacts as part of the project delivery.
* **Controls:** risk & issue management including risk register, risk and control matrix, risk and issue escalation process, and lessons learned log

**Business Tolerance of security risk - how will security risk be managed.**

In the section below, we discuss 1) how the risk tolerance of CCS for the Conclave SSO was built and 2) how risk was managed before and after the build.

**Risk tolerance**: As this project forms the core of all potential platforms within CCS, and therefore Buyers and Supplier dealings across all of Government, security issues cannot and should not be tolerated. We formally assessed the level of risk during the Discovery Phase, but this was limited to reviewing level 3 architecture diagrams, and portions of diagrams covering authentication/ authorisation. Given the platform and data classification and the security risk of this programme the platform should be built using industry best practices in all dimensions of security.

 **Existing platform risk tolerance:** There are over 23 points of entry to the CCS procurement world, each entry point requiring its own individual login identity and password. During our impact analysis of NQC SRS, we highlighted a number of items posing a security risk to CSS which should not be present in the final build of the Conclave solution. The conclusion is that Conclave should set a high bar on acceptable risk tolerance.

**Domain-Driven Design:** Part of our design agreed with CCS is that we incorporate DomainDriven Design and that our solution be completely cloud native. This design requires further effort as during the discovery phase we only began work to introduce concepts such as user input validation which is a topic we have worked extensively on across various domains and clients. All design concepts need to be assessed to ensure acceptable levels of risk are maintained.

**Security certifications:** Brickendon manage risk by having appropriately qualified individuals and are aligned to various security standards. Brickendon is ISO 27001 and CTAR certified, compliant and audited every year. Brickendon adopt many of the best practises set out within the specifications for ISMS and as part of the Conclave solution will apply these practices as early as possible in the project.

**‘Authentication’ and ‘Authorisation’:** Our design has the ‘Authentication’ and

‘Authorisation’ layers requiring separate validation. For user management capabilities we incorporate the ideology that ‘Even a fault-tolerant program could even distrust its own internals.’

Security Design Principles - As set by Technical Design Delivery Authority (TDDA) CCS - how will these be incorporated (especially in any build), proven and adhered to?

Our design is based on the NCSC Cyber Security Principles which can be applied in the following way:

**Establish the context:** Brickendon’s work in the Discovery Phase has identified all potential elements which compose the system. Whilst some elements used in the future may be open source, it is important to monitor for any known vulnerabilities or CVE’s. The key objective here is to avoid blind spots in the design.

**Making compromise difficult:** Best practises (both physical and virtual should be implemented) this should include the relevant firewall rules, network security groups, Web Application firewalls, segregation of data both physically (different VPC for DB’s) and virtual - data-domains (from a physical perspective) and escaping of strings (to remove vulnerabilities such as XSS etc..), MFA etc.. from a software and design perspective.

**Making disruption difficult:** Utilising Cloud Service providers where possible – due to their underlying infrastructure and managed services to prevent these issues.

**Proactive Compromise Detection:** Log everything, any actions, whether user driven, admin driven or application driven should be logged and analysed using many of the available tools.

**Reducing the impact of compromise:** Domain-Driven Design and Segregated Data

Domain’s provide a large amount of protection, other methods include: Encryption in Transit, Encryption at Rest, Secure Database Schema Designs, RBAC etc…

**Secure by Default:** The standard approach is to apply security by default ensuring that additional standards, such as OWASP, Secure Defaults (the experience for users should be secure by default), Principle of Least Privilege/Separation of Duties (Secure Database Schema Designs, RBAC), Principle of Defence in Depth (Tier based validation etc..)

As with all security driven ideologies, it is best to have this audited regularly by a security professional and complete a full Threat Theatre Assessment (Security Assessment)

 Security Assessments are periodic reviews of items that pose the highest risk to the system – in the case of Conclave, as a custom-built solution, any 3rd party libraries as well as integrations with internal and external platforms, should be assessed for known vulnerabilities and categorised by risk. This will also include item’s set up and hosted on the Governments PaaS – where most security risks will be faults due to user error in configuration of resources.

Customer Security Assurance – how will this be managed, be how, proven?

Customer Security assurance ties well with existing GDPR and Secure by Design guidelines. This will be separated out into multiple functions:

**Secure Default:** items such as tenant controlled Multi Factor Authentication (MFA)

**Domain Driven Design:** Data storage segregation based on data domains – certain data will not be grouped.

**Encryption:** Encryption in Transit, Encryption at Rest

Management of the above, will come down to platform owners. These items should be audited annually and recommendations applied.

Security Outcomes – How will they be assured, proven?

Security outcomes are mostly associated with GDPR and the ICO/NCSC guidelines.

This should be treated similar to any other software project as listed below:

* **Organisational Structure and Policies** should be advised upon to manage risk
* **Data governance** through the correct information security policies.
* **Security Risks:** identify and assess potential security risks at points where the system processes personal data (this is limited to the concept of IdP federation – where the current design does NOT synchronise profiles)
* **3rd party processors:** Understanding our reliance and issues arising from 3rd party processors (IdP)
* **Data Security:** apply best practices and adhering to an appropriate data governance framework to ensure data is secure

How will security be integrated within any future system?

The Conclave platform is designed to be a modular, extensible, but otherwise standalone platform. The integration is based on well-known protocols with existing best practises around security and assurance. It is built to support the following protocols:

* OiDC
* oAuth 2.0
* SAML 2.0

How will security testing be conduct? How will this be managed as an ongoing concern? What is the definition of ‘Good’ for security for the system?

At the outset of the engagement we will capture CCS’s unique security requirement as part of the Non-Functional Requirements (NFRs). These NFRs will be detailed and agreed with CCS to enable various tests including security testing to be conducted.

Security testing will be formally planned at the start of the project and will be tested iteratively through the project life cycle in line with standard agile practice. This will be conducted by a suitably qualified professional and should include at a minimum the following activities:

* **Security Scanning:** test of a network's vulnerabilities. A security scan does not attempt to break into the network illegally; rather it tries to find areas of vulnerability.
* **Penetration Testing /Ethically hacking:** engaging a qualified and suitably experienced external party to search for vulnerabilities in the application and try to exploit them. As this is a cloud hosted application, we need the test to include searching for weaknesses in the cloud platform as well as the software application and transit of data between Conclave and Salesforce and Jaeger.
* **Risk Assessment:** assessing the various information assets of CCS which could be used in a cyber-attack. These include: hardware both on premises and cloud hosted, systems, laptops, customer data, and intellectual property. The assessment would then identify the various risks that could affect these assets.
* **Security Audit:** at least annually, the platform or platforms should be evaluated against a set up pre-established criteria.

**Requirements**

**Agree accurate requirements:** The first step and possibly the most import step when providing a robust solution is our best practice requirements gathering process. We ensure that requirements have been gathered, understood and agreed with CCS stakeholders. We look to completely remove the ambiguity around the requirements and make sure the acceptance criteria for each requirement is clearly defined, recorded and understood by all parties. We approach this in an iterative model to ensure that we keep it simple for all stakeholders. This iterative agile process helps us to ensure that the CCS’s requirements are delivered to the highest level of accuracy and on time.

**Translate to clear technology requirements:** After each iteration of producing robust requirements, we will hold mini brainstorming sessions with the development and testing teams to ensure that requirements are clarified from a technology perspective. The requirements will also be continually validated with key stakeholders iteratively. During this process, technology requirements will be clearly analysed and necessary Proof of Concepts

“PoCs” will be built to ensure that the solution is future proofed for later roadmap developments and emerging technologies. Where possible, these POCs will be demonstrated to CCS stakeholders to ensure they meet their requirements.

**Testing:**

**i) Our Principles of Testing**

Brickendon’s award-winning testing team and we have seven (7) key principles of testing. These are:

* **End-to-end Approach:** We approach testing from an end-to-end perspective. As a strong foundation, we focus on strategising all tasks involved in the test design, test execution, end-end testing, defect management, test data, test pre-conditions and deployment process.
* **100% Coverage:** We use innovative methodologies, for example our award nominated Time Check Point System ‘TCPS’(details below) to ensure there is 100% coverage across all areas of testing such as functional, non-functional, operational acceptance, UAT etc., This provides a strong foundation to avoid the defect leakage and production issues as each build goes live.
* **CAD Model**: We build and deploy test deliverables, for example test cases design and execution, and test automation in CAD (Continuous Automation & Deployments) model. In this process we iteratively increase the automation coverage and deploy them for execution.
* **Integrated Automation:** We make sure all automation, management, repository tools are integrated thereby achieving full 100% automated testing and deployment workflow.
* **Easy to enhance and maintain:** We design the test frameworks in such a way that the test coverage can be enhanced by non-technical resources and the end-end framework is easily maintainable.
* **Accelerators & Tooling:** We select the accelerator solutions and right set of tools to make sure we are cost-effective and quicker in the implementations.
* **Automation ROI:** For Automation efforts, we make sure the ROI (Return of Investment) is continuously tracked and improved through the lifecycle of the automation.

**ii) Our High-level Testing Approach (to minimise defects in all phases)**

This section runs you through the approach Brickendon’s award winning team has applied to ensure we have a Testing Approach that minimises defects. This includes:

**Implement Time Check Point System ‘TCPS’:** TCPS is Brickendon’s award-nominated innovative test estimation model. It accurately allocates resources in the test part of any project by building a matrix of complexity and priority to every test case. This delivers high quality functional/SME test.

**TCPS methodology ensure 100% test coverage:** In all business-critical areas, TCPS ensures that the test coverage is 100%. This includes, but is not limited to, additional scenarios for functional and non-functional tests for:

1. Negative test case scenarios,
2. Edge-cases, and
3. Multi-path test scenarios.

**Build automation suite in parallel to test case design:** we build the functional/SME test cases in parallel to test case design with the technologies aligned to CCS’s existing or target technologies and by using our ‘Hybrid’ methodology to ensure:

1. Prioritise UI automation as per business requirements,
2. Collaborate with the in-house team to build the POC for the chosen technology,
3. Easy Parameterization,
4. Iterative coverage increment, and
5. ‘Smaller, Safer & Faster’ delivery model as part of our awarded DevOps implementations.

**Intelligent Regression:** Build intelligent regression testing by implementing our awarded Automatic intelligent Regression Testing ‘AIRT’ methodology. The objective of AIRT methodology is to automatically identify and run the set of test cases based on changes in code, enabling defects to be found and rectified within the SDLC in a faster and safer way. **iii) End goals of our Testing Approach**

The End goal of Brickendon’s awarded testing approach is to give certainty to any release, be it large or small, that it will be delivered without major defects or faults into the production environment. The key benefits are as follows:

* **Safer Releases:** Production of bug free software and implement non-breaking changes to the Production environment.
* **Smaller Releases:** Non-breaking iterative changes to production. Avoid big-bang releases.
* **Faster Time to Market:** Accelerate the release cycle and faster features/changes to support business. This enables us to deliver bug free code at a velocity that a decade ago was unthinkable.
* **Improved Coding Practices:** through tech workshops, POC and continuous iterative improvements.
* **100% CI/CD testing frameworks:** Capability to release smaller, faster changes in a safe way through CI/CD pipelines.
* **Scaling:** Implement strong methodologies and POCs to enable 100% scaling of the approach to future programs and interface teams.
* **KPI based improvements:** examples: Unit test coverage, defect escape rate, failed deployment rate, mean time to issue detection, mean time to issue resolution, etc.
* **Continuous Improvements in Testing:** Enable the developers to continuously improve

the test coverage and methodologies for ‘safer’ and ‘faster’ testing.

Demonstrated benefits to our clients by implementing our award-winning testing methodologies:

* **ONGOING COST SAVINGS:** Brickendon saved HSBC, a bank, $15.3 million in a global e-commerce program across 36 countries. We did this by delivering a robust application suite in secure banking environment with minimal defects and optimised test efforts using our ‘Faster, Safer, Smaller’ approach.
* **ZERO ROLLBACKS:** For HotDeskPlus, a global digital SaaS client with SSO, we have been releasing weekly for over one year. We ensured ‘Zero’ production rollbacks and ‘Zero’ critical production incidents since first go-live
* **FASTER DELIVERY CYCLES:** For a top-tier investment bank, we reduced the regression testing efforts from ‘3 months’ to ‘sub-6 hours’ by implementing our innovative ‘AIRT (Automated Intelligent Regression Testing)’ methodology in their secure environment.
* **END-TO-END AUTOMATION:** Our end-end automation methodologies, we decreased the ‘time to market’ by 94% in a global multi-million digital program at State Street.
* **REDUCED TESTING EFFORT:** HSBC implemented our award-winning automation techniques to exponentially decrease the testing efforts by 80% and thereby increasing the release quality.

Below is a diagram showing the benefits of Brickendon’s QA velocity and our awarded Testing methodology:



Brickendon have successful experience of performing knowledge transfer and handing project artefacts to our clients. At the outset of this engagement, as we did during the Conclave Discovery Phase, we will host a mini workshop with all relevant stakeholders in CCS. This is to explain our iterative handover plan approach which starts from day 1 of the project. The idea of this workshop is to brainstorm the best practices and define the approach of handover at the start of the engagement so from day 1 we are preparing to transfer the knowledge that we acquire in the engagement to CCS.

We will perform the handover in a fully agile/iterative model to keep the handover process robust and simple. This will include transfer of all project documents including:

* **Governance:** documents relating to programme and project planning, capacity planning, quality management and test plans, budgeting, defining roles and responsibilities across the project and wider stakeholder group, completion of the terms of engagement, terms of reference (ToR), and resource skills matrix.
* **Operations:** Programme reporting documents including milestone reporting to plan, status reporting, financial reporting, risk and issue reporting and all other management reports as to effectively manage the deliverables. This includes managing the change control process encompassing change delivery, change management, business impact analysis, quality control, test and implementation plans, resource and programme finance tracking to plan.
* **Tools:** transfer of data stored on our project management, milestone tracking systems (ie JIRA), source repository systems (ie Github) and all others required to perform activities or store artefacts as part of the project delivery.
* **Controls:** risk & issue management including risk register, risk and control matrix, risk and issue escalation process, and lessons learned log
* **Training and handover packs:** specially prepared documents for handing over the project artefacts

In addition to the above key artefacts, throughout the duration of the contract, technical documentation will be updated by the developers and stored in an agreed shared location.

We will hold regular **Show/Tell Sessions** with internal and external stakeholders to explain new features with mock-ups and demonstrations as they progress through the development stages. This will expand the knowledge from the beginning of the project enabling feedback from all impacted by the project and prepare the users for required sign offs at UAT ahead of the finished production product.

The **Operations/Production Support team** will be engaged from the project commencement. This is to ensure they are prepared for their role after the successful Client(s)/stakeholders UAT to handle the production support with full product and support documentation that will be produced, presented and explained to all relevant production support teams.

**A user’s guide/manual will be produced** early in the project and maintained as interactive changes are added to the finished product. New guide/manuals will be given to the other team members with differing levels of technical knowledge to read and provide feedback to the writer. The aim is to ensure that all users will be able to understand and follow the guide/manual.

As part of the **production release handover**, all support teams, levels 1-3, will be provided with technical documentation, diagrams and flowcharts with time given to each team to read and digest the content and access given to environments to all them to familiarise themselves with the new piece of work and features with Q&A sessions conducted to clarify the technical details. The development team will remain available to the support teams after go-live for a pre-agreed period of time

After the demonstration the meeting will be opened to the stakeholders for questions. All questions will be answered either at the time or, if it is a more complicated question or is specific to that type of user, later directly to the person who raised the questions. Written answers will be emailed to all stakeholders attending the meeting where any questions that were not answered will be addressed.

Stakeholders will then cascade this knowledge and all documentation to their team(s).

All knowledge transfer meetings will be recorded allowing us to ensure that no questions or query are left unanswered.

The development team will be available to provide support, help and guidance to all user and support teams after the GoLive for an agreed period of time.

When work has been completed but before GoLive, several stakeholders, previously identified with the client(s) will be invited to attend a series of “Final” Show and Tell meetings. During this time a full demonstration of the new features and/or a new piece of work will be performed.

**Communication Plan**

Our extensive experience has taught us that to be successful an effective communication plan is a must for any project. In the first days we identify the user groups within the organisation who need to be communicated to, how frequently and the most appropriate channel. In addition to formal management project update packs, we set up methods of disseminating information such as SharePoint sites or give access to project repositories to ensure that the most accurate and up to date information is available to those who need it.

Meeting schedule for effect Engagement and Communication

The below schedule of governance forums aligns with the CCS requirements and utilises Brickendon’s proven best practises in managing and delivering complex secure IT projects:

* **AGILE MEETINGS**: depending on project requirements, some meeting are daily, others will be weekly or fortnightly. For this project we wouldn’t run sprints > 14 days o Attendees: project team
	+ Meetings: sprint planning, daily stand up, print reviews and sprint retrospective
* **WEEKLY WORKING GROUPS:** Inform early to implement the change o Attendees: delivery and IT teams, managers, other CCS and 3rd party representation on needs basis
	+ Activities: progress review, project RAIDs, budget tracking, actions logs o Weekly Status Report circulated to all stakeholders o RAIDs identified for escalation as required to the SteerCo
* **MONTHLY STEERING COMMITTEES (SteerCo):** Advise and ensure project delivers o Attendees: delivery managers, senior management and CCS key stakeholders
	+ Ratify Terms of Reference (ToR) and working group decisions, validate objectives, and make other key decisions i.e. change request of Authority. o Review progress to milestones, escalated RAIDs, budget progress and changes, SteerCo actions log
	+ Monthly SteerCo Report circulated to all relevant stakeholders
* **ENTRY/EXIT GATE REVIEWS for each SDLC Phase**: ensure quality of deliverable o Attendees: delivery managers, workstream leads from areas relevant for the

SDLC Phase, senior management as required o Verify if Entry and Exit Criteria are met for the current and next SDLC Phases respectively.

* + Approvals to proceed or advise of need for corrective actions.
	+ Gate outcomes circulated to all relevant stakeholders

**Continuous Improvement Approach**

Brickendon’s awarded teams are always improving our external and internal processes. We hold regular “blue sky” sessions where we ask everyone in the team, which would include CCS stakeholders, to suggest areas for improvement. This can be formal or via informal methods. On a secure IT development project, like CCS Conclave IDAM SSO, once we have identified an area for improvement, we will implement the Plan-Do-Check-Act (PDCA) cycle which has delivered great benefits at other similar client projects. The key components of this methodology are:

* **PLAN:** Identify an opportunity and plan for change.
* **DO:** Implement the change on a small scale.
* **CHECK:** Use data to analyse the results of the change and determine whether it made a difference.
* **ACT:** If the change was successful, implement it on a wider scale and continuously assess your results. If the change did not work, begin the cycle again.

As with all continuous improvement models we aim to emphasize employee involvement and teamwork. This is to measure and systematise processes, reduce variations, defects, and cycle times. This applies to both our team and the wider stakeholder group from CCS who will be keep fully informed and engaged in this process to ensure it has satisfied the success criteria defined during the first days of the project.

Ultimately, the best processes for CI (Continuous improvement) evolve naturally during the lifecycle of development. As our team members are further integrated into the CCS organisation, we can articulate the higher-level goals of CCS as lower level requirements are delivered in the early phases of the project. Once the PDCA cycle has delivered an enhancement to a system or process we leverage training and workshops to inform the wider CCS community of the change and its benefits. The key components of our continuous improvement training cycle are:

* **EVERYONE:** After agreement with CCS, we believe that training shouldn’t be limited to a certain set of users or user groups. We provide access to training courses and everyone is encouraged to learn new technologies and methodologies.
* **DEVELOPERS:** Developers are encouraged to both enhance their development skills and the user challenges. They are encouraged to use the training in a proactive way, develop mock-ups and proposals to present to CCS for consideration.
* **TESTERS:** Depending on the available CCS environments and applicable software installations, testers are encouraged post the training to look for the most appropriate set ups to automate regression and end user testing saving the CCS time and money.
* **SUPPORT TEAM:** Further training offers the team an opportunity to enhance their customer service skills allowing them to better communicate with CCS’s internal and external clients.

# Schedule 3 - Statement of Work (SOW), including pricing arrangements and Key Staff

#  Sch 3.1 SOW Details

|  |  |
| --- | --- |
| **Date of SOW:** | *02-November-2020* |
| **SOW Reference:** | *DOS-xxx.* |
| **Buyer:** | *Buyer Full Name* |
| **Supplier:** | *Supplier Full Name* |
| **Release Type(s):** | *Please enter here (Release Type(s) can be Adhoc, Inception, Calibration or Delivery)* |
| **Phase(s) of Development:** | *Choose an item (Phase(s) can be Discovery, Alpha, Beta or Live)* |
| **Release Completion Date:** | *Please enter the Release Completion Date* |
| **Duration of SOW** | *Please enter the number of days here* |
| **Charging Method(s) for this Release:** | *Choose an item** *Fixed price*

 |

3.1.1 The Parties will execute a SOW for each Release. Note that any ad-hoc Service requirements are to be treated as individual Releases in their own right (in addition to the Releases at the delivery stage); and the Parties should execute a separate SOW in respect of each.

3.1.2 The rights, obligations and details agreed by the Parties and set out in this SOW apply only in relation to the Services that are to be delivered under this SOW and will not apply to any other SOW’s executed or to be executed under this Call-Off Contract unless otherwise agreed by the Parties.

# Sch 3.2 Key Staff

3.2.1 The Parties agree that the Key Staff in respect of this Project are detailed in the table below.

3.2.2 Table of Key Staff:

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** | **Details** |
|   |   |   |

# Sch 3.3 Deliverables

3.3.1 To be added in agreement between the Buyer and Supplier

# Sch 3.4 Call-Off Contract Charges

3.4.1. For each individual Statement of Work (SOW), the applicable Call-OffContract Charges (in accordance with the charging method in the Order Form) will be calculated using all of the following:

* the agreed relevant rates for Supplier staff or facilities, which are inclusive of any applicable expenses and exclusive of VAT and which were submitted to the Buyer during the Further Competition that resulted in the award of this Call-Off Contract.
* the number of days, or pro rata for every part of a day, that Supplier staff or facilities will be actively providing the Services during the term of the SOW.
* a contingency margin of up to 20% applied to the sum calculated on the basis of the above two points, to accommodate any changes to the SOW Deliverables during the term of the SOW. The Supplier must obtain prior written approval from the Buyer before applying any contingency margin.

3.4.2 The Supplier will provide a detailed breakdown of rates based on time and materials Charges, inclusive of expenses and exclusive of VAT, with sufficient detail to enable the Buyer to verify the accuracy of the time and material Call-Off Contract Charges incurred.

The detailed breakdown for the provision of Services during the term of the SOW will include (but will not be limited to):

* a role description per Supplier Staff;
* a facilities description;
* the agreed relevant rate per day;
* any expenses charged per day, which are in line with the Buyer’s expenses policy (if applicable);
* the number of days, or pro rata for every part day, they will be actively providing the Services during the term of the SOW; and
* the total cost per role/facility

The Supplier will also provide a summary which is to include:

* Total value of this SOW
* Overall Call-Off Contract value
* Remainder of value under overall Call-Off Contract Charge

 Where:

Remainder of value under overall Call-Off Contract Charge = overall Call-Off Contract value - sum of total value of all SOWs invoiced

* Whether there is any risk of exceeding Overall Call-Off Contract value (and thereby requiring a Contract Change Note (CCN) to continue delivery of Services)

3.4.3 If a capped or fixed price has been agreed for a SOW:

* The Supplier will continue at its own cost and expense to provide the Services even where the agreed price has been exceeded; and
* The Buyer will have no obligation or liability to pay for the cost of any Services delivered relating to this order after the agreed price has been exceeded.

3.4.4 Risks or contingencies will be included in the Charges. The Parties agree that the following assumptions, representations, risks and contingencies will apply in relation to the Charges. [Insert full details of any assumptions, representations, risks and contingencies which the Parties are relying on in relation to the Charges].

3.4.5 Any changes to the Supplier Staff (not applicable to Lot 3 Services) should be agreed with the Buyer and covered by a separate SOW where it cannot be accommodated within an existing SOW.

3.4.6 Multiple SOWs can operate concurrently.

3.4.7 The Supplier will keep accurate records of the time spent by the Supplier staff in providing the services and will provide records to the Buyer for inspection on request (not applicable to Lot 3 Services)

#  Sch 3.5. Call-Off Contract Extension Period

# Where the Buyer has specified an Extension Period in the Order Form, the Parties agree that an Extension Period of up to 25% of the initial Call-Off Contract Period can be added to the term of the Call-Off Contract, to accommodate any changes to the Deliverables, or delay in meeting the Buyer’s requirements. The Buyer must give the Supplier the minimum notice specified in the Order Form that an Extension Period is required, set out how long the Extension Period is to be, and obtain prior written approval from the Supplier before applying any Extension Period to the Call-Off Contract period.

# Sch 3.6. Agreement of statement of works

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| BY SIGNING this SOW, the Parties agree to be bound by the terms and conditions set out herein:

|  |
| --- |
| **For and on behalf of the Supplier:** |
| Name and title |  |
| Signature and date |   |

|  |
| --- |
| **For and on behalf of the departmental Buyer:** |
| Name and title |  |
| Signature and date |   |

Please note that this is the first SOW. If the value of the first SOW is lower than the overall Call-Off Contract value, and subsequent SOW(s) are required to ensure the Services are delivered, they must be raised and signed by the Buyer and the Supplier, with a copy sent to CCS for its records.If you exceed the overall Call-Off Contract value and Supplier Staff are still required to deliver the services, then a contract change note (CCN) must be raised, explaining the reason(s) for the extension. |

# Schedule 4 - Contract Change Notice (CCN) – not needed

~~Order Form reference for the Call-Off Contract being varied:~~

~~BETWEEN:~~

|  |
| --- |
| **~~Buyer Full Name~~** ~~("~~**~~the Buyer"~~**~~)~~~~and~~**~~Supplier Full Name~~** ~~(~~**~~"the Supplier"~~**~~)~~ |

1. ~~The Call-Off Contract is varied as follows and shall take effect on the date signed by both Parties:~~

***~~Guidance Note: Insert full details of the change including:~~***

***~~Reason for the change;~~***

***~~Full Details of the proposed change;~~***

***~~Likely impact, if any, of the change on other aspects of the Call-Off Contract;~~***

1. ~~Words and expressions in this Contract Change Notice shall have the meanings given to them in the Call-Off Contract.~~
2. ~~The Call-Off Contract, including any previous changes shall remain effective and unaltered except as amended by this change.~~

**~~Signed by an authorised signatory for and on behalf of the Buyer~~**

|  |  |
| --- | --- |
| ~~Signature:~~ |  |
| ~~Date:~~ | ~~Click here to enter a date.~~ |
| ~~Name:~~ | ~~Click here to enter text.~~ |
| ~~Address:~~ | ~~Click here to enter text.~~ |
|  |  |

**~~Signed by an authorised signatory to sign for and on behalf of the Supplier~~**

|  |  |
| --- | --- |
| ~~Signature:~~ |  |
| ~~Date:~~ | ~~Click here to enter a date.~~ |
| ~~Name:~~ | ~~Click here to enter text.~~ |
| ~~Address:~~ | ~~Click here to enter text.~~ |

# Schedule 5 - Balanced Scorecard

In addition to the Supplier’s performance management obligations set out in the Framework Agreement, the Parties may agree to the following Balanced Scorecard & KPIs for this Call-Off Contract (see Balanced Scorecard Model below):



The purpose of the Balanced Scorecard is to promote contract management activity, through measurement of a Supplier’s performance against Key Performance Indicators, which the Buyer and Supplier should agree at the beginning of a Call-Off Contract. The targets and measures listed in the example scorecard (above) are for guidance and should be changed to meet the agreed needs of the Buyer and Supplier.

The recommended process for using the Balanced Scorecard is as follows:

1. The Buyer and Supplier agree a templated Balanced Scorecard together with a performance management plan, which clearly outlines the responsibilities and actions that will be taken if agreed performance levels are not achieved.
2. On a pre-agreed schedule (e.g. monthly), both the Buyer and the Supplier provide a rating on the Supplier’s performance
3. Following the initial rating, both Parties meet to review the scores and agree an overall final score for each Key Performance Indicator
4. Following agreement of final scores, the process is repeated as per the agreed schedule

CCS encourages Buyers to share final scores with CCS, so that performance of the Framework Agreement can be monitored. This may be done by emailing scores to: cloud\_digital@crowncommercial.gov.uk.

# Schedule 6 - Optional Buyer terms and conditions

# Sch 6.1 Buyer’s agent

The Buyer (as principal) has authorised [NAME OF AGENT] to act as agent on their behalf. The Buyer (as principal) remains liable for all of the Buyer obligations under this Call-Off Contract entered into on its behalf by its agent.

# Schedule 7 - How Services are bought (Further Competition process)

Services are bought under this Call-Off Contract using the Further Competition process set out in Section 3 of the Framework Agreement (How Services will be bought).

# Schedule 8 - Deed of guarantee – not needed

~~[This section should be completed where a deed of guarantee is part of the buyer’s needs. Securing a deed of guarantee may have cost implications and the buyer should consider the appropriateness of seeking one. The relevant sections below should be completed based on the details of the winning supplier.]~~

**~~This deed of guarantee~~** ~~is made on [insert date date/month/year ] 20[ ]~~ **~~between~~**~~:~~

~~(1) [Insert the name of the guarantor] a company incorporated in England and Wales with number [insert company no.] whose registered office is at [insert details of the~~~~guarantor's registered office here] [OR] [a company incorporated under the Laws of [insert country], registered in [insert country] with number [insert number] at [insert place of registration], whose principal office is at [insert office details]~~~~(~~**~~'guarantor'~~**~~); in favour of~~

**~~and~~**

~~(2) THE BUYER whose offices are XXXXXXXXXXXXXXXXX (~~**~~‘Beneficiary’~~**~~)~~

**~~Whereas~~**~~:~~

~~(A) The guarantor has agreed, in consideration of the Buyer entering into the Call-Off Contract with the Supplier, to guarantee all of the Supplier's obligations under the Call-Off Contract.~~

~~(B) It is the intention of the Parties that this document be executed and take effect as a deed.~~

~~In consideration of the Buyer entering into the Call-Off Contract, the Guarantor hereby agrees with the Buyer as follows:~~

**~~DEFINITIONS AND INTERPRETATION~~**

~~In this deed of guarantee, unless defined elsewhere in this deed of guarantee or the context requires otherwise, defined terms will have the same meaning as they have for the purposes of the Call-Off Contract.~~

|  |  |
| --- | --- |
| **~~‘Call-Off Contract’~~** | ~~means [the Guaranteed Agreement] made between the Buyer and the Supplier on [insert date]~~ |
| **~~'Guaranteed Obligations'~~** | ~~means all obligations and liabilities of the Supplier to the Buyer under the Call-Off Contract together with all obligations owed by the Supplier to the Buyer that are supplemental to, incurred under, ancillary to or calculated by reference to the Call-Off Contract~~ |

~~References to this deed of guarantee and any provisions of this deed of guarantee or to any other document or agreement (including to the Call-Off Contract) apply now, and as amended, varied, restated, supplemented, substituted or novated in the future.~~

~~Unless the context otherwise requires, words importing the singular are to include the plural and vice versa.~~

~~References to a person are to be construed to include that person's assignees or transferees or successors in title, whether direct or indirect.~~

~~The words ‘other’ and ‘otherwise’ are not to be construed as confining the meaning of any following words to the class of thing previously stated where a wider construction is possible.~~

~~Unless the context otherwise requires, reference to a gender includes the other gender and the neuter.~~

~~Unless the context otherwise requires, references to an Act of Parliament, statutory provision or statutory instrument also apply if amended, extended or re-enacted from time to time.~~

~~Unless the context otherwise requires, any phrase introduced by the words ‘including’, ‘includes’, ‘in particular’, ‘for example’ or similar, will be construed as illustrative and without limitation to the generality of the related general words.~~

~~References to Clauses and Schedules are, unless otherwise provided, references to Clauses of and Schedules to this deed of guarantee.~~

~~References to liability are to include any liability whether actual, contingent, present or future.~~

**~~Guarantee and indemnity~~**

~~The Guarantor irrevocably and unconditionally guarantees that the Supplier duly performs all of the guaranteed obligations due by the Supplier to the Buyer.~~

~~If at any time the Supplier will fail to perform any of the guaranteed obligations, the Guarantor irrevocably and unconditionally undertakes to the Buyer it will, at the cost of the Guarantor:~~

* ~~fully perform or buy performance of the guaranteed obligations to the Buyer~~
* ~~as a separate and independent obligation and liability, compensate and keep the Buyer compensated against all losses and expenses which may result from a failure by the Supplier to perform the guaranteed obligations under the Call-Off Contract~~

~~As a separate and independent obligation and liability, the Guarantor irrevocably and unconditionally undertakes to compensate and keep the Buyer compensated on demand against all losses and expenses of whatever nature, whether arising under statute, contract or at common Law, if any obligation guaranteed by the guarantor is or becomes unenforceable, invalid or illegal as if the obligation guaranteed had not become unenforceable, invalid or illegal provided that the guarantor's liability will be no greater than the Supplier's liability would have been if the obligation guaranteed had not become unenforceable, invalid or illegal.~~

**~~Obligation to enter into a new Contract~~**

~~If the Call-Off Contract is terminated or if it is disclaimed by a liquidator of the Supplier or the obligations of the Supplier are declared to be void or voidable, the Guarantor will, at the request of the Buyer enter into a Contract with the Buyer in the same terms as the Call-Off Contract and the obligations of the Guarantor under such substitute agreement will be the same as if the Guarantor had been original obligor under the Call-Off Contract or under an agreement entered into on the same terms and at the same time as the Call-Off Contract with the Buyer.~~

**~~Demands and notices~~**

~~Any demand or notice served by the Buyer on the Guarantor under this deed of guarantee will be in writing, addressed to:~~

~~[Address of the Guarantor in England and Wales]~~

~~[Email address of the Guarantor representative]~~

~~For the Attention of [insert details]~~

~~or such other address in England and Wales as the Guarantor has from notified to the Buyer in writing as being an address for the receipt of such demands or notices.~~

~~Any notice or demand served on the Guarantor or the Buyer under this deed of guarantee will be deemed to have been served:~~

* ~~if delivered by hand, at the time of delivery~~
* ~~if posted, at 10am on the second Working Day after it was put into the post~~
* ~~if sent by email, at the time of despatch, if despatched before 5pm on any Working Day, and in any other case at 10am on the next Working Day~~

~~In proving Service of a notice or demand on the Guarantor or the Buyer, it will be sufficient to prove that delivery was made, or that the envelope containing the notice or demand was properly addressed and posted as a prepaid first class recorded delivery letter, or that the fax message was properly addressed and despatched.~~

~~Any notice purported to be served on the Buyer under this deed of guarantee will only be valid when received in writing by the Buyer.~~

**~~BENEFICIARY'S PROTECTIONS~~**

~~The Guarantor will not be discharged or released from this deed of guarantee by:~~

* ~~any arrangement made between the Supplier and the Buyer (whether or not such arrangement is made with the assent of the Guarantor)~~
* ~~any amendment to or termination of the Call-Off Contract~~
* ~~any forbearance or indulgence as to payment, time, performance or otherwise granted by the Buyer (whether or not such amendment, termination, forbearance or indulgence is made with the assent of the Guarantor)~~
* ~~the Buyer doing (or omitting to do) anything which, but for this provision, might exonerate the Guarantor~~

~~This deed of guarantee will be a continuing security for the Guaranteed Obligations and accordingly:~~

* ~~it will not be discharged, reduced or otherwise affected by any partial performance (except to the extent of such partial performance) by the Supplier of the Guaranteed Obligations or by any omission or delay on the part of the Buyer in exercising its rights under this deed of guarantee~~
* ~~it will not be affected by any dissolution, amalgamation, reconstruction, reorganisation, change in status, function, control or ownership, insolvency, liquidation, administration, appointment of a receiver, voluntary arrangement, any legal limitation or other incapacity, of the Supplier, the Buyer, the Guarantor or any other person~~
* ~~if, for any reason, any of the Guaranteed Obligations is void or unenforceable against the Supplier, the Guarantor will be liable for that purported obligation or liability as if the same were fully valid and enforceable and the Guarantor were principal debtor~~
* ~~the rights of the Buyer against the Guarantor under this deed of guarantee are in addition to, will not be affected by and will not prejudice, any other security, guarantee, indemnity or other rights or remedies available to the Buyer~~

~~The Buyer will be entitled to exercise its rights and to make demands on the Guarantor under this deed of guarantee as often as it wishes. The making of a demand (whether effective, partial or defective) relating to the breach or non-performance by the Supplier of any Guaranteed Obligation will not preclude the Buyer from making a further demand relating to the same or some other Default regarding the same Guaranteed Obligation.~~

~~The Buyer will not be obliged before taking steps to enforce this deed of guarantee against the Guarantor to:~~

* ~~obtain judgment against the Supplier or the Guarantor or any third party in any court~~
* ~~make or file any claim in a bankruptcy or liquidation of the Supplier or any third party~~
* ~~take any action against the Supplier or the Guarantor or any third party~~
* ~~resort to any other security or guarantee or other means of payment.~~

~~No action (or inaction) by the Buyer relating to any such security, guarantee or other means of payment will prejudice or affect the liability of the Guarantor.~~

~~The Buyer's rights under this deed of guarantee are cumulative and not exclusive of any rights provided by Law. The Buyer’s rights may be exercised as often as the Buyer deems expedient.~~

~~Any waiver by the Buyer of any terms of this deed of guarantee, or of any Guaranteed Obligations, will only be effective if given in writing and then only for the purpose and upon the terms and conditions on which it is given.~~

~~Any release, discharge or settlement between the Guarantor and the Buyer will be conditional upon no security, disposition or payment to the Buyer by the Guarantor or any other person being void, set aside or ordered to be refunded following any enactment or Law relating to liquidation, administration or insolvency or for any other reason. If such condition will not be fulfilled, the Buyer will be entitled to enforce this deed of guarantee subsequently as if such release, discharge or settlement had not occurred and any such payment had not been made. The Buyer will be entitled to retain this security before and after the payment, discharge or satisfaction of all monies, obligations and liabilities that are or may become due owing or incurred to the Buyer from the Guarantor for such period as the Buyer may determine.~~

**~~GUARANTOR INTENT~~**

~~Without prejudice to the generality of Clause 5 (The Buyer’s protections), the Guarantor expressly confirms that it intends that this deed of guarantee will extend from time to time to any variation, increase, extension or addition of or to the Call-Off Contract and any associated fees, costs or expenses.~~

**~~RIGHTS OF SUBROGATION~~**

~~The Guarantor will, at any time when there is any Default in the performance of any of the Guaranteed Obligations by the Supplier or any Default by the Guarantor in the performance of any of its obligations under this deed of guarantee, exercise any rights it may have:~~

* ~~of subrogation and indemnity~~
* ~~to take the benefit of, share in or enforce any security or other guarantee or indemnity for the Supplier’s obligations~~
* ~~to prove in the liquidation or insolvency of the Supplier~~

~~The Guarantor will do this in accordance with the Buyer’s written instructions and will hold any amount recovered as a result of the exercise of such rights on trust for the Buyer and pay the same to the Buyer on first demand.~~

~~The Guarantor acknowledges that it has not taken any security from the Supplier in connection with this deed of guarantee and agrees not to do so until Beneficiary receives all monies payable hereunder and will hold any security taken in breach of this Clause on trust for the Buyer.~~

**~~DEFERRAL OF RIGHTS~~**

~~Until all amounts which may be or become payable by the Supplier under, or in connection with, the Call-Off Contract have been irrevocably paid in full, the Guarantor agrees that, without the prior written consent of the Buyer, it will not:~~

* ~~exercise any rights it may have to be indemnified by the Supplier~~
* ~~claim any contribution from any other guarantor of the Supplier’s obligations under the Call-Off Contract~~
* ~~take the benefit (in whole or in part and whether by way of subrogation or otherwise) of any rights of the Buyer under the Call-Off Contract or of any other guarantee or security taken following, or in connection with, the Call-Off Contract~~
* ~~demand or accept repayment in whole or in part of any indebtedness now or hereafter due from the Supplier~~
* ~~claim any set-off or counterclaim against the Supplier~~

~~If the Guarantor receives any payment or other benefit or exercises any set-off or counterclaim or otherwise acts in breach of this Clause 8, anything so received and any benefit derived directly or indirectly by the Guarantor therefrom will be held on trust for the Buyer and applied in or towards discharge of its obligations to the Buyer under this deed of guarantee.~~

**~~REPRESENTATIONS AND WARRANTIES~~**

~~The Guarantor hereby represents and warrants to the Buyer that:~~

* ~~the Guarantor is duly incorporated and is a validly existing company under the Laws of its place of incorporation~~
* ~~has the capacity to sue or be sued in its own name~~
* ~~the Guarantor has power to carry on its business as now being conducted and to own its Property and other assets~~
* ~~the Guarantor has full power and authority to execute, deliver and perform its obligations under this deed of guarantee and no limitation on the powers of the Guarantor will be exceeded as a result of the Guarantor entering into this deed of guarantee~~
* ~~the execution and delivery by the Guarantor of this deed of guarantee and the performance by the Guarantor of its obligations under this deed of guarantee including entry into and performance of a Call-Off Contract following Clause 3) have been duly authorised by all necessary corporate action and do not contravene or conflict with:~~
* ~~the Guarantor's memorandum and articles of association or other equivalent constitutional documents, any existing Law, statute, rule or Regulation or any judgment, decree or permit to which the Guarantor is subject~~
* ~~the terms of any agreement or other document to which the Guarantor is a party or which is binding upon it or any of its assets~~
* ~~all governmental and other authorisations, approvals, licences and consents, required or desirable~~

~~This deed of guarantee is the legal valid and binding obligation of the Guarantor and is enforceable against the Guarantor in accordance with its terms.~~

**~~PAYMENTS AND SET-OFF~~**

~~All sums payable by the Guarantor under this deed of guarantee will be paid without any set-off, lien or counterclaim, deduction or withholding, except for those required by Law. If any deduction or withholding must be made by Law, the Guarantor will pay that additional amount to ensure that the Buyer receives a net amount equal to the full amount which it would have received if the payment had been made without the deduction or withholding.~~

~~The Guarantor will pay interest on any amount due under this deed of guarantee at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgment.~~

~~The Guarantor will reimburse the Buyer for all legal and other costs (including VAT) incurred by the Buyer in connection with the enforcement of this deed of guarantee.~~

**~~GUARANTOR'S ACKNOWLEDGEMENT~~**

~~The Guarantor warrants, acknowledges and confirms to the Buyer that it has not entered into this deed of guarantee in reliance upon the Buyer nor been induced to enter into this deed of guarantee by any representation, warranty or undertaking made by, or on behalf of the Buyer, (whether express or implied and whether following statute or otherwise) which is not in this deed of guarantee~~

**~~ASSIGNMENT~~**

~~The Buyer will be entitled to assign or transfer the benefit of this deed of guarantee at any time to any person without the consent of the Guarantor being required and any such assignment or transfer will not release the Guarantor from its liability under this Guarantee.~~

~~The Guarantor may not assign or transfer any of its rights or obligations under this deed of guarantee.~~

**~~SEVERANCE~~**

~~If any provision of this deed of guarantee is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision will be severed and the remainder of the provisions will continue in full force and effect as if this deed of guarantee had been executed with the invalid, illegal or unenforceable provision eliminated.~~

**~~THIRD-PARTY RIGHTS~~**

~~A person who is not a Party to this deed of guarantee will have no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this deed of guarantee. This Clause does not affect any right or remedy of any person which exists or is available otherwise than following that Act.~~

**~~GOVERNING LAW~~**

~~This deed of guarantee, and any non-Contractual obligations arising out of or in connection with it, will be governed by and construed in accordance with English Law.~~

~~The Guarantor irrevocably agrees for the benefit of the Buyer that the courts of England will have jurisdiction to hear and determine any suit, action or proceedings and to settle any dispute which may arise out of or in connection with this deed of guarantee and for such purposes hereby irrevocably submits to the jurisdiction of such courts.~~

~~Nothing contained in this Clause will limit the rights of the Buyer to take proceedings against the Guarantor in any other court of competent jurisdiction, nor will the taking of any such proceedings in one or more jurisdictions preclude the taking of proceedings in any other jurisdiction, whether concurrently or not (unless precluded by applicable Law).~~

~~The Guarantor irrevocably waives any objection which it may have now or in the future to the courts of England being nominated for this Clause on the ground of venue or otherwise and agrees not to claim that any such court is not a convenient or appropriate forum.~~

~~[The Guarantor hereby irrevocably designates, appoints and empowers [the Supplier] [a suitable alternative to be agreed if the Supplier's registered office is not in England or Wales] either at its registered office or on fax number [insert fax no.] from time to time to act as its authorised agent to receive notices, demands, Service of process and any other legal summons in England and Wales for the purposes of any legal action or proceeding brought or to be brought by the Buyer in respect of this deed of guarantee. The Guarantor hereby irrevocably consents to the Service of notices and demands, Service of process or any other legal summons served in such way.]~~

~~IN WITNESS whereof the Guarantor has caused this instrument to be executed and delivered as a Deed the day and year first before written.~~

~~EXECUTED as a DEED by~~

***~~[Insert name of the Guarantor]~~*** ~~acting by~~ ***~~[Insert/print names]~~***

~~Director~~

~~Director/Secretary~~

# Schedule 9 - Processing, Personal Data and Data Subjects

**Subject matter of the processing:**

The supplier will receive staff details for the purposes of establishing user/admin permissions within the new site, and will utilize Supplier names and key contacts when populating information about CCS Frameworks.

**Duration of the processing:**

Processing under this contract will take place from the [insert date] 2020, for 25 weeks.

**Nature and purposes of the processing:**

Development and implementation of a system to manage user accounts and sign-on for an unlimited number of CCS and wider Government systems (all current and future CCS systems, with additional consideration for wider government services)

**Type of Personal Data:**

Name, Title, email address, organisation

**Categories of Data Subject:**

Staff (including volunteers, agents, and temporary workers), Suppliers

**Plan for return or destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data:**

Data will be transferred to CCS upon conclusion of the contract.

# Schedule 10 – Alternative Clauses

Not Applicable.