**Framework Schedule 1 (Specification)**

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make available to all Buyers under this Framework Contract.

The Supplier must only provide the Deliverables for the Lot that they have been appointed to.

For all Lots and/or Deliverables, the Supplier must help Buyers comply with any specific applicable Standards of the Buyer.

The Deliverables and any Standards set out in clause 1 below may be refined (to the extent permitted and set out in the Order Form) by a Buyer during a Further Competition Procedure to reflect its Deliverables requirements for entering into a particular Call-Off Contract.



  

**Framework Schedule 2 (Framework Tender)**

[Redacted]

**Framework Schedule 3 (Framework Prices)**

1. How Framework Prices are used to calculate Call-Off Charges
   1. The Framework Prices:
      1. will be used as the basis for the charges (and are maximums that the Supplier may charge) under each Call Off Contract; and
      2. cannot be increased except as in accordance with this Schedule.
   2. The Charges:
      1. shall be calculated in accordance with the terms of the Call Off Contract and in particular in accordance with the terms of the Order Form;
      2. cannot be increased except as specifically permitted by the Call Off Contract and in particular shall only be subject to Indexation where specifically stated in the Order Form
   3. Any variation to the Charges payable under a Call Off Contract must be agreed between the Supplier and the Buyer and implemented using the same procedure for altering Framework Prices in accordance with the provisions of this Framework Schedule 3.
2. How Framework Prices are calculated
   1. The pricing mechanisms and prices set out in Annex 1 shall be available for use in calculation of Framework Prices in Call Off Contracts.
3. Are costs and expenses are included in the Framework Prices
   1. Except as expressly set out in Paragraph 4 below, or otherwise stated in a Call Off Order Form the Framework Prices shall include all costs and expenses relating to the provision of Deliverables. No further amounts shall be payable in respect of matters such as:
      1. incidental expenses such as travel, subsistence and lodging, document or report reproduction, shipping, desktop or office equipment costs, network or data interchange costs or other telecommunications charges; or
      2. costs incurred prior to the commencement of any Call Off Contract.
4. When the Supplier can ask to change the Framework Prices
   1. The Framework Prices will be fixed for the first 12 months following the Framework Contract Commencement Date (the date of expiry of such period is a "**Review Date**"). After this Framework Prices can only be adjusted on each following yearly anniversary (the date of each such anniversary is also a "**Review Date**").
   2. The Supplier shall give CCS at least three (3) Months' notice in writing prior to a Review Date where it wants to request an increase. If the Supplier does not give notice in time then it will only be able to request an increase prior to the next Review Date.
   3. Any notice requesting an increase shall include:
      1. a list of the Framework Prices to be reviewed;
      2. for each Framework Price under review, written evidence of the justification for the requested increase including:
         1. a breakdown of the profit and cost components that comprise the relevant Framework Price;]
         2. details of the movement in the different identified cost components of the relevant Framework Price;
         3. reasons for the movement in the different identified cost components of the relevant Framework Price;
         4. evidence that the Supplier has attempted to mitigate against the increase in the relevant cost components; and
         5. evidence that the Supplier’s profit component of the relevant Framework Price is no greater than that applying to Framework Prices using the same pricing mechanism as at the Contract Commencement Date.
   4. CCS shall consider each request for a price increase. CCS may grant Approval to an increase at its sole discretion.
   5. Where CCS approves an increase then it will be implemented from the first (1st) Working Day following the relevant Review Date or such later date as CCS may determine at its sole discretion and Annex 1 shall be updated accordingly.
5. Other events that allow the Supplier to change the Framework Prices
   1. The Framework Prices can also be varied (and Annex 1 will be updated accordingly) due to:
      1. a Specific Change in Law in accordance with Clause 24;
      2. a review in accordance with insurance requirements in Clause 13;
      3. a benchmarking review in accordance with Call Off Schedule 16 (Benchmarking)]
      4. a request from the Supplier, which it can make at any time, to decrease the Framework Prices; and
      5. indexation, where Annex 1 states that a particular Framework Price or any component is “subject to Indexation” in which event

**Table 1:**

[Redacted]

**Annex 1: Supplier’s Charging Structure**

Table 1:

[Redacted]

**Framework Schedule 4 (Framework Management)**

1. Definitions
   1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

|  |  |
| --- | --- |
| Supplier Framework Manager | 1. has the meaning given to it in Paragraph 3.1 of this Schedule; and |
| Supplier Review Meetings | 1. has the meaning given to it in Paragraph 3.2 of this Schedule. |

1. How CCS and the Supplier will work together
   1. The successful delivery of this Contract will rely on the ability of the Supplier and CCS to develop a strategic relationship immediately following the conclusion of this Contract and maintaining this relationship throughout the Framework Contract Period.
   2. To achieve this strategic relationship, there will be a requirement to adopt proactive framework management activities which will be informed by quality Management Information, and the sharing of information between the Supplier and CCS.
   3. This Schedule outlines the general structures and management activities that the Parties shall follow during the Framework Period.
2. Framework Management
   1. **Framework Management Structure**
      1. The Supplier shall provide a suitably qualified nominated contact (the "Supplier Framework Manager") who will take overall responsibility for delivering the Deliverables required within this Contract, as well as a suitably qualified deputy to act in their absence.
      2. The Supplier shall put in place a structure to manage this Contract in accordance with Framework Schedule 1 (Specification) and the Performance Indicators.
      3. A governance structure will be agreed between the Parties as soon as reasonably practicable following the Framework Start Date.
      4. Following discussions between the Parties following the Framework Start Date, where requested by CCS, the Supplier shall produce and issue to CCS a draft Supplier Action Plan. CCS shall not unreasonably withhold or delay its agreement to the draft Supplier Action Plan. The Supplier Action Plan shall be agreed between the Parties and come into effect within two (2) weeks from receipt by the Supplier of the draft Supplier Action Plan.
      5. The Supplier Action Plan shall be maintained and updated on an ongoing basis by CCS. Any changes to the Supplier Action Plan shall be notified by CCS to the Supplier. The Supplier shall not unreasonably withhold its agreement to any changes to the Supplier Action Plan. Any such changes shall, unless CCS otherwise Approves, be agreed between the Parties and come into effect within two weeks from receipt by the Supplier of CCS’s notification.
      6. The Supplier agrees to comply with its obligations in the Supplier Action Plan as updated from time to time.
      7. The Supplier shall comply with all requests from CCS in regard to compliance requirements as required including:
         1. D&B risk failure score monitoring;
         2. regular evidence that the Required Insurances and Additional Insurances have been renewed and maintained;
         3. invoice payment performance; and
         4. verification of required accreditations & certifications.
      8. Suppliers should participate in further competitions when identified as part of the final bidder list. Failure to bid on further competitions without an acceptable reason may result in the Supplier being suspended from the Framework, in accordance with Clause 10.8 (Partially ending and suspending the contract) of the Core Terms, for a period as decided by CCS.
   2. **Supplier Review Meetings**
      1. Regular performance review meetings will take place at CCS’s premises throughout the Framework Contract Period ("Supplier Review Meetings") at such times and frequencies as CCS determine from time to time (which are anticipated to be once every Month or less). The Parties shall be flexible about the timings of these meetings.
      2. The Supplier Review Meetings will review the Supplier’s performance under this Contract and, where applicable, the Supplier’s adherence to the Supplier Action Plan. The agenda for each Supplier Review Meeting shall be set by CCS and sent to the Supplier in advance.
      3. The Supplier Review Meetings shall be attended, as a minimum, by CCS Representative(s) and the Supplier Framework Manager.

[Guidance Note to bidders: for further information on Supplier Action Plans and Supplier’s management see the "Supplier Guidance on Supplier Management" published by CCS at:

<https://www.gov.uk/government/publications/crown-commercial-service-supplier-logo-and-brand-guidelines>]

1. **How the Supplier’s Performance will be measured**
   1. The Supplier’s performance will be measured by the following Performance Indicators (“PI”):

|  |  |  |  |
| --- | --- | --- | --- |
| **Performance Indicator (PI)** | | **PI Target** | **Measured by** |
| 1.1 | All Management Information returns to be returned to CCS by the 7th working day of each month | 100% accuracy in terms of completeness of income, timeliness | Confirmation of time of receipt by CCS (as evidenced within the CCS’s data warehouse (MISO) system) |
| 1.2 | All valid CCS invoices to be paid within 30 calendar days of issue | 100% Accuracy, timeliness | Confirmation of receipt and time of receipt by CCS (as evidenced within CCS’s CODA system) |
| 1.3 | Supplier self-audit certificate to be issued to CCS in accordance with the Framework Agreement | 100% Accuracy, timeliness | Confirmation of receipt and time of receipt by CCS |
| 1.4 | Actions identified in an Audit Report to be delivered by the dates set out in the Audit | 100% Accuracy, timeliness | Confirmation of receipt and time of receipt by CCS |

* 1. The Supplier shall comply with the PIs and establish processes to monitor its performance against them and the Supplier’s achievement of PIs shall be reviewed during the Supplier Review Meetings.
  2. CCS reserves the right to adjust, introduce new, or remove PIs throughout the Framework Contract Period, however any significant changes to PIs shall be agreed between CCS and the Supplier in accordance with the Variation Procedure.
  3. CCS reserves the right to use and publish the performance of the Supplier against the PIs without restriction.

1. **What the Supplier must do to measure their performance**
   1. The Supplier shall cooperate in good faith with CCS to develop efficiency tracking performance measures for this Contract. This shall include the following (but this list is not exhaustive and may be developed during the Framework Contract Period):
      1. tracking reductions in product volumes and product costs, in order to demonstrate that Buyers are consuming less and buying more smartly; and
      2. developing additional PIs to ensure that this Contract supports the emerging target operating model across central government (particularly in line with centralised sourcing and category management, procurement delivery centres and payment processing systems and shared service centres).
   2. The metrics that are to be implemented to measure efficiency shall be developed and agreed between CCS and the Supplier. Such metrics shall be incorporated into the list of PIs set out in this Schedule.
   3. The ongoing progress and development of the efficiency tracking performance measures shall be reported through framework management activities as outlined in this Schedule.
2. **What to do if CCS and the Buyer can’t agree about the performance** 
   1. In the event that CCS and the Supplier are unable to agree the performance score for any PI during a Supplier Review Meeting, the disputed score shall be recorded and the matter shall be referred to CCS Representative and the Supplier Authorised Representative in order to determine the best course of action to resolve the matter (which may involve organising an ad-hoc meeting to discuss the performance issue specifically).
   2. In cases where CCS Representative and the Supplier Authorised Representative fail to reach a solution within a reasonable period of time, the matter shall be referred to the Dispute Resolution Procedure.
3. **Marketing**
   1. The Supplier shall ensure that a person is appointed as Marketing Contact who shall be responsible for the marketing obligations of the Supplier in relation to this Contract.
   2. **How the Supplier must contribute to CCS publications**
      1. The Supplier shall supply current information relating to the Deliverables it offers for inclusion in CCS marketing materials when required by CCS from time to time.
      2. Such information shall be provided in such form and at such time as CCS may request.
      3. Failure to comply with the provisions of Paragraphs 7.2.1 and 7.2.2 may result in the Supplier's exclusion from the use of such marketing materials.
   3. **What Suppliers can say in its own publications**
      1. All marketing materials produced by the Supplier in relation to this Framework shall at all times comply with the CCS branding guidance at: [https://www.gov.uk/government/publications/crown-commercial-service-supplier-logo-and-brand-guidelines](ttps://www.gov.uk/government/publications/crown-commercial-service-supplier-logo-and-brand-guidelines).
      2. The Supplier will periodically update and revise its marketing materials to ensure ongoing compliance.
      3. The Supplier shall regularly review the content of any information which appears on its website and which relates to each Contract and ensure that such information is up to date at all times.
      4. The Supplier shall obtain all appropriate approvals prior to publishing any content in relation to a Contract with that Party using any media, including on any electronic medium, and the Supplier will ensure that such content is regularly maintained and updated. In the event that the Supplier fails to maintain or update the content, CCS or the relevant Buyer may give the Supplier notice to rectify the failure and if the failure is not rectified its reasonable satisfaction within one (1) Month of receipt of such notice, and shall have the right to remove such content itself or require that the Supplier immediately arranges the removal of such content.
4. **Where CCS might oversee parts of the Call-Off Contract**
   1. CCS shall have oversight of certain processes which are operated under Call-Off Contracts. Such oversight shall be provided in relation to the operation of the following schedules (**"Supported Schedules"**) in each Call-Off Contract:

* Call-Off Schedule 3 (Continuous Improvement);
* Call-Off Schedule 8 (Business Continuity and Disaster Recovery);
* Call-Off Schedule 9 (Security); and
* Call-Off Schedule 16 (Benchmarking).
  1. **How the Supplier must support CCS involvement**
     1. The Supplier shall co-operate as reasonably required by CCS in relation to the Supported Schedules including:
* provision of information;
* allowing CCS to act as agent for the Buyers under the Supported Schedules for such matters as CCS may notify to the Supplier from time to time; and
* such other matters as CCS may notify to the Supplier from time to time.
  1. **Where CCS might manage the process for Buyers collectively** 
     1. In addition to general oversight as referred to above the following specific oversight shall apply to the individual Supported Schedules:
        1. Call-Off Schedule 3 (Continuous Improvement) - the Supplier shall:
* adopt a policy of continuous improvement in relation to the Deliverables; and
* create, maintain and update a continuous improvement plan for improving the provision of the Deliverables and/or reducing the Charges and, where requested by CCS, incorporate any improvement identified in accordance with the Variation Procedure.
  + - 1. Call-Off Schedule 8 (Business Continuity and Disaster Recovery) - the Supplier shall:
* create and hold a template BCDR plan that can be used by each Buyer and shall make it available to CCS so that it can be published to potential Buyers; and
* notify CCS in the event of the invocation or potential invocation of any BCDR plan and the Supplier shall provide such support as CCS may reasonably require to coordinate the application of BCDR plans across all Call Off Contracts.
  + - 1. Call-Off Schedule 9 (Security) - the Supplier shall:
* create and hold a template Security Plan that can be used by each Buyer and shall make it available to CCS so that it can be published to potential Buyers; and
* notify CCS in the event of breach of any Security Plan and the Supplier shall provide such support as CCS may reasonably require to coordinate the application of Security Plans across all Call Off Contracts.
  + - 1. Call-Off Schedule 16 (Benchmarking)- the Supplier:
* shall notify CCS in the event that any bench marker is appoint in respect of any Call-Off Contract and the Supplier recognises that CCS may want to co-ordinate how benchmarking is conducted across multiple Call-Off Contracts;
* shall where CCS is appointed as agent by Buyers in respect of benchmarking, co-operate with CCS in order to operate the benchmarking as efficiently as possible;
* agrees that notwithstanding the remainder of Clause 15 (Confidentiality) in the Core Terms, CCS shall be entitled to publish the results of any benchmarking of the Charges to Other Buyers (subject to the other party entering into reasonable confidentiality undertakings).

**Framework Schedule 5 (Management Charges and Information)**

1. **How to provide management information to CCS**
   1. The Supplier shall, at no charge, provide timely, full, accurate and complete MI Reports to CCS which incorporate the data, in the correct format, required by the MI Reporting Template and such guidance that CCS may issue from time to time.
   2. The initial MI Reporting Template is set out in the Annex to this Schedule and CCS may change it from time to time (including the data required and/or format) and issue a replacement version. CCS shall give at least thirty (30) days' notice in writing of any such change and shall specify the date from which it must be used. The Supplier may not make any amendment to the current MI Reporting Template without the prior Approval of CCS. The Supplier shall include in the MI Reports and the volume of expenditure undertaken with SMEs by the Supplier and its Subcontractors in the delivery of this Contract and each Call-Off Contract.
2. **Reporting Periods**
   1. MI Reports must be completed (even where there are no transactions to report) and returned to CCS by the Reporting Date every Month during the Framework Period and thereafter, until all transactions relating to Call-Off Contracts have permanently ceased.
   2. The MI Report should report (among other things) on Orders received and transactions occurring during the Month to which it regardless of when the work was actually completed. For example, if an invoice is raised for October but the work was actually completed in September, the Supplier must report the invoice in October's MI Report and not September's. Each Order received by the Supplier must be reported only once when the Order is received.
   3. If the Supplier discovers any errors in any reported Management Information then it will inform CCS and provide corrections in the next MI Report.
3. **Submitting the information**
   1. MI Reports shall be completed electronically and uploaded to the CCS Management Information System Online (MISO) available at: <https://miso.ccs.cabinetoffice.gov.uk/> in accordance with the instructions provided in MISO.
   2. CCS may (acting reasonably) require that MI Reports be submitted by an alternative means (such as email).
   3. The Supplier shall, where requested by CCS, supply Management Information to a Buyer as specified by CCS.
4. **How CCS can use the Management Information**
   1. The Supplier grants CCS a non-exclusive, transferable, perpetual, irrevocable, royalty free licence to:
      1. use and to share with any Buyer, Other Contracting Authority and Relevant Person; and/or
      2. publish (subject to any information that is exempt from disclosure in accordance with the provisions of FOIA being redacted),
      3. any Management Information supplied to CCS for CCS’ normal operational activities including administering this Contract and/or all Call-Off Contracts, monitoring public sector expenditure, identifying savings or potential savings and planning future procurement activity.
   2. CCS may consult with the Supplier to inform its decision to publish information however CCS shall retain absolute discretion regarding the extent, content and format of any disclosure.
5. **Paying the Management Charge**
   1. Following receipt of the completed MI Report CCS shall invoice the Supplier for the Management Charge payable for the Month to which the MI report relates.
   2. The Management Charge excludes VAT which is payable on provision of a valid VAT invoice.
   3. The Supplier shall pay CCS the Management Charges (and other charges payable in accordance with this Schedule) in cleared funds within thirty (30) days of receipt by the Supplier of an undisputed invoice to such bank or building society account set out in the invoice.
6. **What happens if the Management Information is wrong**
   1. Following an MI Failure CCS may issue reminders to the Supplier or require the Supplier to rectify it. The Supplier shall rectify any deficient or incomplete MI Report as soon as possible and not more than five (5) Working Days following receipt of any such reminder.
   2. **Meetings**
      1. The Supplier agrees to attend meetings between the Parties in person to discuss the circumstances of any MI Failure(s) at the request of CCS. If CCS requests such a meeting the Supplier shall propose and document measures to ensure that the MI Failures are rectified and do not occur in the future as a supplement to the Management Charge.
   3. **Admin fees** 
      1. If, in any rolling three (3) Month period, two (2) or more MI Failures occur, the Supplier acknowledges and agrees that CCS shall have the right to invoice the Supplier Admin Fees in respect of any MI Failures as they arise in subsequent Months.
      2. The Supplier acknowledges and agrees that the Admin Fees are a fair reflection of the additional costs incurred by CCS as a result of the Supplier failing to supply Management Information as required by this Contract.
7. **What happens if the Management Charge isn’t paid**
   1. If two (2) MI Failures occur in any rolling six (6) Month period then an "**MI Default**" shall be deemed to have occurred and CCS shall be entitled to:
      1. charge and the Supplier shall pay an additional default management charge ("Default Management Charge") in respect of the Months in which the MI failure occurred and subsequent Months in which they continue, calculated in accordance with Paragraph 7.2; and/or
      2. terminate this Contract.
   2. The Default Management Charge shall be the higher of:
      1. the average Management Charge paid or payable by the Supplier in the previous six (6) Month period or, if the MI Default occurred within less than six (6) Months from the commencement date of the first Call-Off Contract, in the whole period preceding the date on which the MI Default occurred; or
      2. the sum of five hundred pounds (£500).
   3. If the Supplier provides sufficient Management Information to rectify any MI Failures to the satisfaction of CCS and the Management Information demonstrates that:
      1. the Supplier has overpaid the Management Charges as a result of the application of the Default Management Charge then the Supplier shall be entitled to a refund of the overpayment, net of any Admin Fees where applicable; or
      2. the Supplier has underpaid the Management Charges during the period when a Default Management Charge was applied, then CCS shall be entitled to immediate payment of the balance as a debt together with interest.

**Annex: MI Reporting Template**

[Redacted]

**Framework Schedule 6 (Order Form Template and Call-Off Schedules)**

**Part A**

**Order Form Template**

CALL-OFF REFERENCE: **[Insert** Buyer’s contract reference number]

THE BUYER: **[Insert** Buyer’s name]

BUYER ADDRESS [**Insert** business address]

THE SUPPLIER: [**Insert** name of Supplier]

SUPPLIER ADDRESS:[**Insert** registered address (if registered)]

REGISTRATION NUMBER:[**Insert** registration number (if registered)]

DUNS NUMBER: **[Insert** if known]

SID4GOV ID: **[Insert** if known]

**[Buyer guidance:** This Order Form, when completed and executed by both Parties, forms a Call-Off Contract. A Call-Off Contract can be completed and executed using an equivalent document or electronic purchase order system. If an electronic purchasing system is used instead of signing as a hard-copy, the text below must be   
copied into the electronic order form]

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated [**Insert** date of issue].

It’s issued under the Framework Contract with the reference number [**Insert** Framework Contract Reference number] for the provision of [**Insert** name of goods and services].

CALL-OFF LOT(S):

**[Insert** the relevant lot numbers **or insert** Not applicable]

CALL-OFF INCORPORATED TERMS

The following documents are incorporated into this Call-Off Contract. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) for RM6101
3. The following Schedules in equal order of precedence:

[**Buyer guidance: delete** any highlighted Schedules that you do not need for this Call-Off Contract. **Add** any additional Schedule needed, providing it is within scope of the framework agreement. **Remove** any highlighting remaining before finalising this Order Form. **Remove** this guidance too.]

* Joint Schedules for **RM6101**
  + Joint Schedule 2 (Variation Form)
  + Joint Schedule 3 (Insurance Requirements)
  + Joint Schedule 4 (Commercially Sensitive Information)
  + Joint Schedule 6 (Key Subcontractors)
  + Joint Schedule 7 (Financial Difficulties)
  + Joint Schedule 8 (Guarantee)
  + Joint Schedule 9 (Minimum Standards of Reliability) – Not Used
  + Joint Schedule 10 (Not used)
  + Joint Schedule 11 (Processing Data)
* Call-Off Schedules for **[Insert** Call-Off reference number]
  + Call-Off Schedule 1 (Transparency Reports)
  + Call-Off Schedule 2 (Staff Transfer)
  + Call-Off Schedule 3 (Continuous Improvement)
  + Call-Off Schedule 5 (Pricing Details)
  + Call-Off Schedule 6 (ICT Services)
  + Call-Off Schedule 7 (Key Supplier Staff)
  + Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
  + Call-Off Schedule 9 (Security)
  + Call-Off Schedule 10 (Exit Management)
  + Call-Off Schedule 11 (Installation Works)
  + Call-Off Schedule 12 (Clustering)
  + Call-Off Schedule 13 (Implementation Plan and Testing)
  + Call-Off Schedule 14 (Service Levels)
  + Call-Off Schedule 15 (Call-Off Contract Management)
  + Call-Off Schedule 16 (Benchmarking)
  + Call-Off Schedule 17 (MOD Terms)
  + Call-Off Schedule 18 (Background Checks)
  + Call-Off Schedule 19 (Scottish Law)
  + Call-Off Schedule 20 (Call-Off Specification)

1. CCS Core Terms (version 3.0.2)
2. Joint Schedule 5 (Corporate Social Responsibility) for RM6101
3. Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

**Part B**

**Call-Off Schedules**

****

Framework Schedule 7 (Call-Off Award Procedure)

Part 1: Order Procedure

1. **How a Call-Off Contract is awarded**
   1. If a potential Buyer decides to source Deliverables through this Contract then it will award its Deliverables in accordance with the procedure in this Schedule and the requirements of the Regulations. The award may be made directly to the Supplier or with a Supplier’s appointed dealer and in either case the Supplier shall remain fully responsible under the terms of this Framework Contract and Call-Off Contract for the supply of the Deliverables to the Buyer or Requesting Body.
   2. If the potential Buyer can determine that:
      1. its Deliverables can be met by the Suppliers’ catalogues and description of the Deliverables as set out in Framework Schedule 1 (Specification) and Framework Schedule 2 (Framework Tender); and
      2. all of the terms of the proposed Call-Off Contract are laid down in this Contract and do not require amendment or any supplementary terms and conditions;

then the Buyer may award a Call-Off Contract in accordance with the procedure set out in Paragraph 5 below.

* 1. If all of the terms of the proposed Call-Off Contract are not laid down in this Contract and the potential Buyer:
     1. requires the Supplier to develop proposals or a solution in respect of such Deliverables; and/or
     2. needs to amend or refine the terms of the Framework Contract to reflect its Deliverables to the extent permitted by and in accordance with the Regulations;

then the Buyer shall award a Call-Off Contract in accordance with the Further Competition Procedure set out in Paragraph 7 below.

1. Direct award – when you don’t need further competition
   1. Subject to clause 1.2 above the Buyer awarding a Call-Off Contract under this Contract without holding a further competition shall:
      1. develop a clear Statement of Requirements;
      2. apply the Direct Award Criteria to the Suppliers’ catalogues and description of the Deliverables as set out in Framework Schedule 1 (Specification) and Framework Schedule 2 (Framework Tender) for all Suppliers capable of meeting the Statement of Requirements in order to establish which Supplier provides the most economically advantageous solution; and
      3. on the basis set out above, award the Call-Off Contract with the successful Supplier in accordance with Paragraph 7 below.
2. How a further competition works

What the Buyer has to do

* 1. The Buyer awarding a Call-Off Contract under this Contract through a Further Competition Procedure shall:
     1. develop a Statement of Requirements setting out its requirements for the Deliverables and identify the Suppliers capable of supplying the them;
     2. amend or refine the Deliverables to reflect its requirements by using the Order Form only to the extent permitted by and in accordance with the requirements of the Regulations;
     3. invite tenders by conducting a Further Competition Procedure for its Deliverables in accordance with the Regulations and in particular:
        1. if an Electronic Reverse Auction (as defined in Paragraph 4 below) is to be held, the Buyer shall notify the Suppliers identified in accordance with clause 3.1.1 and shall conduct the Further Competition Procedure in accordance with the procedures set out in Paragraph 4; or
        2. if an Electronic Reverse Auction is not used, the Buyer shall:
           1. invite the Suppliers identified in accordance with clause 3.1.1 to submit a tender in writing for each proposed Call-Off Contract to be awarded by giving written notice by email to the relevant Supplier Representative of each Supplier;
           2. set a time limit for the receipt by it of the tenders which takes into account factors such as the complexity of the subject matter of the proposed Call-Off Contract and the time needed to submit tenders; and
           3. keep each tender confidential until the time limit set out for the return of tenders has expired.
     4. apply the Further Competition Award Criteria to the Suppliers' compliant tenders submitted through the Further Competition Procedure as the basis of its decision to award a Call-Off Contract for its Deliverables;
     5. on the basis set out above, award its Call-Off Contract to the successful Supplier in accordance with Paragraph 7. The Call-Off Contract shall:
        1. state the Deliverables;
        2. state the tender submitted by the successful Supplier;
        3. state the charges payable for the Deliverables in accordance with the tender submitted by the successful Supplier; and
        4. incorporate the terms of the Order Form and Contract (as may be amended or refined by the Buyer in accordance with Paragraph 3.1.2. above) applicable to the Deliverables,
     6. provide unsuccessful Suppliers with written feedback in relation to the reasons why their tenders were unsuccessful.

What the Supplier has to do

* 1. The Supplier shall in writing, by the time and date by the time and date specified by the Buyer following an invitation to tender pursuant to Paragraph 3.1.3 above, provide CCS and the Buyer with either:
     1. a statement to the effect that it does not wish to tender in relation to the Deliverables; or
     2. the full details of its tender made in respect of the relevant Statement of Requirements. In the event that the Supplier submits such a tender, it should include, as a minimum:
        1. an email response subject line to comprise unique reference number and Supplier name, so as to clearly identify the Supplier;
        2. a brief summary, in the email (followed by a confirmation letter), stating that the Supplier is bidding for the Statement of Requirements;
        3. a proposal covering the Deliverables;
        4. CVs of key staff – as a minimum any lead consultant, with others, as considered appropriate along with required staff levels (if necessary); and
        5. confirmation of discounts applicable to the Deliverables, as referenced in Framework Schedule 3 (Framework Charges) (if applicable).
     3. The Supplier shall ensure that any prices submitted in relation to a Further Competition Procedure held pursuant to this Paragraph 3 shall be based on the Charging Structure and take into account any discount to which the Buyer may be entitled as set out in Framework Schedule 3 (Framework Charges).
     4. The Supplier agrees that:
        1. all tenders submitted by the Supplier in relation to a Further Competition Procedure held pursuant to this Paragraph 4 shall remain open for acceptance by the Buyer for ninety (90) Working Days (or such other period specified in the invitation to tender issued by the Buyer in accordance with the Call-Off Procedure); and
        2. all tenders submitted by the Supplier are made and will be made in good faith and that the Supplier has not fixed or adjusted and will not fix or adjust the price of the tender by or in accordance with any agreement or arrangement with any other person. The Supplier certifies that it has not and undertakes that it will not:
           1. communicate to any person other than the person inviting these tenders the amount or approximate amount of the tender, except where the disclosure, in confidence, of the approximate amount of the tender was necessary to obtain quotations required for the preparation of the tender; and
           2. enter into any arrangement or agreement with any other person that he or the other person(s) shall refrain from submitting a tender or as to the amount of any tenders to be submitted.

1. **How e-Auctions work**
   1. Where indicated in the Order Form, the Buyer shall be entitled to include a reverse auction in the Further Competition Procedure in accordance with the rules laid down by the Buyer and the Regulations.
   2. Where the Buyer wishes to undertake an electronic reverse auction, where Suppliers compete in real time by bidding as the auction unfolds ("Electronic Reverse Auction") then before undertaking it, the Buyer will make an initial full evaluation of all tenders received in response to its Statement of Requirements. The Buyer will then invite to the Electronic Reverse Auction only those tenders that are admissible in accordance with the Regulations. The invitation shall be accompanied by the outcome of the full initial evaluation of the relevant tenders.
   3. The Buyer will inform the Suppliers of the specification for the Electronic Reverse Auction which shall include:
      * 1. the information to be provided at auction, which must be expressed in figures or percentages of the specified quantifiable features;
        2. the mathematical formula to be used to determine automatic ranking of bids on the basis of new prices and/or new values submitted;
        3. any limits on the values which may be submitted;
        4. a description of any information which will be made available to Suppliers in the course of the Electronic Reverse Auction, and when it will be made available to them;
        5. the conditions under which Suppliers will be able to bid and, in particular, the minimum differences which will, where appropriate, be required when bidding;
        6. relevant information concerning the electronic equipment used and the arrangements and technical specification for connection;
        7. subject to clause 4.5, the date and time of the start of the Electronic Reverse Auction; and
        8. details of when and how the Electronic Reverse Auction will close.
   4. The Electronic Reverse Auction may not start sooner than two (2) Working Days after the date on which the specification for the Electronic Reverse Auction has been issued.
   5. Throughout each phase of the Electronic Reverse Auction the Buyer will communicate to all Suppliers sufficient information to enable them to ascertain their relative ranking.
   6. The Supplier acknowledges and agrees that:
      * 1. the Buyer and its officers, servants, agents, group companies, assignees and customers (including CCS) do not guarantee that its access to the Electronic Reverse Auction will be uninterrupted or error-free;
        2. its access to the Electronic Reverse Auction may occasionally be restricted to allow for repairs or maintenance; and
        3. it will comply with all such rules that may be imposed by the Buyer in relation to the operation of the Electronic Reverse Auction.
   7. The Buyer will close the Electronic Reverse Auction on the basis of:
      * 1. a date and time fixed in advance;
        2. when no new prices or values meeting the minimum differences required pursuant to Paragraph 4.3(e) have been received within the prescribed elapsed time period; or
        3. when all the phases have been completed.
2. No requirement to award
   1. Notwithstanding the fact that the Buyer has followed a procedure as set out above in Paragraph 2 or 3 (as applicable), the Supplier acknowledges and agrees that the Buyer shall be entitled at all times to decline to make an award for its Deliverables and that nothing in this Contract shall oblige the Buyer to award any Call-Off Contract.
3. Who is responsible for the award
   1. The Supplier acknowledges that the Buyer is independently responsible for the conduct of its award of Call-Off Contracts under this Contract and that CCS is not responsible or accountable for and shall have no liability whatsoever, except where it is the Buyer, in relation to:
      1. the conduct of Buyer in relation to this Contract; or
      2. the performance or non-performance of any Call-Off Contracts between the Supplier and Buyer entered into pursuant to this Contract.
4. Awarding and creating a Call-Off Contract
   1. Subject to Paragraphs 1 to 6 above, a Buyer may award a Call-Off Contract with the Supplier or the Supplier’s appointed dealer by sending (including electronically) a signed order form substantially in the form (as may be amended or refined by the Buyer in accordance with Paragraph 3.1.2 above) of the Order Form Template set out in Framework Schedule 6 (Order Form Template and Call-Off Schedules).
   2. The Parties agree that any document or communication (including any document or communication in the apparent form of a Call-Off Contract) which is not as described in this Paragraph 7 shall not constitute a Call-Off Contract under this Contract.
   3. On receipt of an order form as described in Paragraph 7.1 from a Buyer the Supplier shall accept the Call-Off Contract by promptly signing and returning (including by electronic means) a copy of the order form to the Buyer concerned.
   4. On receipt of the countersigned Order Form from the Supplier, the Buyer shall send (including by electronic means) a written notice of receipt to the Supplier within two (2) Working Days and the Call Off Contract shall be formed with effect from the Call Off Start Date stated in the Order Form.

**Part 2: Award Criteria**

1. This Part 2 is designed to assist Buyers seeking to award a Call-Off Contract on the basis of direct award or through reopening competition under a Further Competition Procedure in accordance with the Call-Off Procedure.
2. A Call-Off Contract shall be awarded on the basis of most economically advantageous tender (**"MEAT"**) from the point of view of the Buyer.
3. This Schedule includes details of the evaluation criteria and any weightings that will be applied to that criteria. Criteria applicable to a direct award are set out at Annex A to this Schedule, and criteria applicable to a Further Competition Procedure are set out in Annex B to this Schedule.

Annex A: Direct award criteria

The following criteria and weightings shall be applied to the Suppliers' compliant tenders submitted through direct award.

|  |  |  |
| --- | --- | --- |
| **Criteria Number** | **Criteria - ranked in order of importance** | **Percentage Weightings (or rank order of importance where applicable) – to be set by the Buyer conducting the direct award** |
| 1 | Price (life cycle costs, cost effectiveness & price; price and running costs) | 0-100% |
| 2 | Technical merit; coverage, network capacity and performance as specified in relevant service levels  Quality (including delivery time, sales service, good value, accessories, service fitness for purpose) | 0-100% |

Annex B: Further Competition Award Criteria

The following criteria shall be applied to the Deliverables set out in the Suppliers' compliant tenders submitted through the Further Competition Procedure:

|  |  |  |
| --- | --- | --- |
| **Criteria Number** | **Criteria** | **Percentage Weightings (or rank order of importance where applicable) – to be set by the Buyer conducting the further competition** |
| 1 | Price (life cycle costs, cost effectiveness & price; price and running costs) | 0-100% |
| 2 | Technical merit; coverage, network capacity and performance as specified in relevant service levels  Quality (including delivery time, sales service, good value, accessories, service fitness for purpose) | 0-100% |

**Framework Schedule 8 (Self Audit Certificate)**

Dear [name]

In accordance with Clause 6 (Record keeping and reporting) of the Framework Contract entered into on 3rd December 2018 between [CCS to insert name of Supplier] and the CCS, we confirm the following:

1. In our opinion based on the testing undertaken [name of Supplier] has in place suitable systems for identifying and recording the transactions taking place under the provisions of the above Framework Contract.

2. We have tested the systems for identifying and reporting on Framework Contract activity and found them to be operating satisfactorily.

3. We have tested a sample of [CCS to insert number of sample transactions that must tested]] Orders and related invoices during our audit for the financial year ended [Supplier to insert financial year] and confirm that they are correct and in accordance with the terms and conditions of the Framework Contract.

4. We have tested from the order processing and invoicing systems a sample of [CCS to insert number of sample transactions that must tested] public sector orders placed outside the Framework Contract during our audit for the financial year ended [Supplier to insert financial year] and confirm they have been identified correctly as orders placed outside the Framework Contract an appropriate and legitimately tendered procurement route has been used to place those orders, and those orders should not otherwise have been routed via centralised and mandated procurement processes executed by CCS.

5. We have also attached an Audit Report which provides details of the methodology applied to complete the review, the sampling techniques applied, details of any issues identified and remedial action taken.

Name:………………………………………………………

Signed:…………………………………………………...…

[Head of Internal Audit/ Finance Director/ External Audit firm]

Date:……………………………………………………….

Professional Qualification held by Signatory:............................................................

**Framework Schedule 9 (Cyber Essentials Scheme)**

1. **Definitions**
   1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

|  |  |
| --- | --- |
| **"Cyber Essentials Scheme"** | means the Cyber Essentials Scheme developed by the Government which provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet based threats (as may be amended from time to time). Details of the Cyber Essentials Scheme can be found here: <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview>; |
| **"Cyber Essentials Basic Certificate"** | means the certificate awarded on the basis of self-assessment, verified by an independent certification body, under the Cyber Essentials Scheme and is the basic level of assurance; |
| **"Cyber Essentials Certificate"** | means Cyber Essentials Basic Certificate to be provided by the Supplier as set out in the Framework Award Form |
| **"Cyber Essential Scheme Data"** | means sensitive and personal information and other relevant information as referred to in the Cyber Essentials Scheme; and |
| **"Cyber Essentials Plus Certificate"** | means the certification awarded on the basis of external testing by an independent certification body of the Supplier’s cyber security approach under the Cyber Essentials Scheme and is a more advanced level of assurance. |

1. **What Certification do you need**
   1. Where the Framework Award Form requires that the Supplier provide a Cyber Essentials Certificate prior to the framework commencement date, the Supplier shall provide a valid Cyber Essentials Certificate, then on or prior to the framework commencement date the Supplier must have delivered to CCS evidence of the same. Where the Supplier fails to comply with this clause it shall be prohibited from commencing the provision of Deliverables under any Contract until such time as the Supplier has evidenced to CCS its compliance with this Paragraph 2.1.
   2. Where the Supplier continues to process OFFICIAL Data during the Contract Period of any Call-Off Contract the Supplier shall deliver to CCS evidence of renewal of the Cyber Essentials Certificate on each anniversary of the first applicable certificate obtained by the Supplier under Paragraph 2.1.
   3. Where the Supplier is due to Process OFFICIAL Data after the Start date of the first Call-Off Contract but before the end of the Framework Period or Contact Period of the last Call-Off Contract, the Supplier shall deliver to CCS evidence of:
      1. a valid and current Cyber Essentials PLUS Certificate before the Supplier Processes any such Cyber Essentials Scheme Data; and
      2. renewal of the valid Cyber Essentials PLUS Certificate on each anniversary of the first Cyber Essentials Scheme PLUS certificate obtained by the Supplier under Paragraph 2.1.
   4. In the event that the Supplier fails to comply with Paragraphs 2.2 or 2.3 (as applicable), CCS reserves the right to terminate this Contract for material Default.
   5. The Supplier shall ensure that all Sub-Contracts with Subcontractors who Process OFFICIAL Data contain provisions no less onerous on the Subcontractors than those imposed on the Supplier under this Contract in respect of the Cyber Essentials Scheme under Paragraph 2.1 of this Schedule.
   6. This Schedule shall survive termination or expiry of this Contract and each and any Call-Off Contract.

**Framework Schedule 10 (NOT USED)**

**Framework Schedule 11 (Security)**

1. Definitions
   1. In this Schedule the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

|  |  |
| --- | --- |
| "Breach of Security" | 1. means the occurrence of:    1. any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Authority and/or the Supplier in connection with this Contract; and/or    2. the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Authority and/or the Supplier in connection with this Contract, 2. in either case as more particularly set out in the security requirements in the Security Policy; |
| "ISMS" | 1. the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and |
| "Security Tests" | 1. tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security. |

1. Introduction
   1. This Schedule sets out:
      1. the principles which the Supplier shall comply with when performing its obligations under this Agreement in order to ensure the security of the Authority Data, the IT Environment, the Supplier Solution and the Service;
      2. the process which shall apply to the Accreditation of the Service in Paragraph 4;
      3. the Certification Requirements applicable to the Service and wider delivery organisation in Paragraph 9;
      4. the Security Tests which the Supplier shall conduct during the Term in Paragraph 10;
      5. the Security Tests which the Authority may conduct during the Term in Paragraph 10;
      6. the requirements to proactively manage vulnerabilities in the Service in Paragraph 13;
      7. the obligations on the Supplier to manage the security risks associated with malicious action on or against the eSourcing Service and to scan for vulnerabilities, contain the spread of, and minimise the impact of Malicious code when introduced into the eSourcing Service Paragraph 12; and
      8. each Party's obligations in the event of an actual or attempted Breach of Security in Paragraph 12.
2. Principles of Security
   1. The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Authority Data and, consequently on the security of:
      1. the IT Environment;
      2. the Supplier Solution;
      3. the eSourcing Information Management System; and
      4. the Authority information whilst that Authority Data is under the control of the Supplier or any of its Sub-contractors.
   2. The eSourcing Security Working Group shall, in addition to its responsibilities set out in Schedule 4 (Framework Management), monitor and may also provide recommendations to the Authority on the Accreditation of the eSourcing Service.
   3. Each Party shall provide access to members of its information assurance personnel to facilitate the Supplier's design, implementation, operation, management and continual improvement of the eSourcing Risk Management Documentation and the security of the Supplier Solution and eSourcing Service and otherwise at reasonable times on reasonable notice.
3. Statement of Information Risk Appetite and Baseline Security Requirements
   1. The Supplier acknowledges that the Authority has provided and the Supplier has received a statement of information risk appetite (the "**Statement of Information Risk Appetite**"). for the Service.
   2. The Authority's Baseline Security Requirements in respect of the Service are set out in Annex 1.
   3. The eSourcing Service shall be subject to Security Assurance in accordance with this Paragraph 5.
   4. The Accreditation shall be performed by the Authority or by representatives appointed by the Authority.
   5. Prior to the Operational Services Commencement Date, the Supplier shall prepare and submit to the Authority the Risk Management Documentation for the Service, which shall comply with, and be subject to approval by the Authority in accordance with, this Paragraph 6 (the "**eSourcing Risk Management Documentation**").
   6. The eSourcing Risk Management Documentation shall address the requirements detailed in Section 4 which will detail the security risk position for the eSourcing service and provide appropriate detail to enable the Authority to determine that the level of residual risk is within the Authority’s risk appetite.
   7. If the eSourcing Risk Management Documentation submitted to the Authority pursuant to Paragraph 6 is approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the eSourcing Risk Management Documentation is not approved by the Authority, the Supplier shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the eSourcing Risk Management Documentation following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this Paragraph may be unreasonably withheld or delayed. However, any failure to approve the eSourcing Risk Management Documentation on the grounds that it does not comply with the requirements set out in Paragraph 5.7 shall be deemed to be reasonable.
   8. To facilitate Accreditation of the eSourcing Service, the Supplier shall provide the Authority and its authorised representatives with:
      1. access to the Sites, ICT information assets and ICT systems within the Service on request or in accordance with the Accreditation Plan; and
      2. such other information and/or documentation that the Authority or its authorised representatives may reasonably require, to enable the Authority to establish that the Service is compliant with the eSourcing Risk Management Documentation.
   9. The Authority shall, by the relevant date set out in the Security Management Plan, review the identified risks to the Service and issue to the Supplier either:
      1. The Authority to Operate statement which will then form part of the eSourcing Risk Management Documentation, confirming that the Authority is satisfied that the identified risks to the Service have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Authority ; or
      2. a rejection notice stating that the Authority considers that the residual risks to the Service have not been reduced to a level acceptable by the Authority and the reasons why (**"Risk Management Rejection Notice"**).
   10. If the Authority issues a Risk Management Rejection Notice, the Supplier shall, within ten (10) Working Days of the date of the Risk Management Rejection Notice:
       1. address all of the issues raised by the Authority in such notice; and
       2. notify the Authority that the Service is ready for an Security Assurance Decision.
   11. If the Authority determines that the Supplier's actions taken pursuant to the Risk Management Rejection Notice have not reduced the residual risks to the Core Service to an acceptable level and issues a further Risk Management Rejection Notice, the failure to receive a Risk Management Approval Statement shall constitute a material Default and the Authority may by terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 15.
   12. The process set out in Paragraphs 4.8 and 4.9 shall be repeated until such time the Authority issues an Authority to Operate to the Supplier or terminates this Agreement.
   13. The Supplier acknowledges that it shall not be permitted to use the Service to Process Authority Data prior to receiving an Authority to Operate statement.
   14. The Supplier shall keep the eSourcing Risk Management Documentation under review and shall update it annually in accordance with this Paragraph and the Authority shall review the Accreditation Decision annually and following the occurrence of any of the events set out in Paragraph 4.15.
   15. The Supplier shall notify the Authority within five (5) Working Days after becoming aware of:
       1. a significant change to the components or architecture of the Service;
       2. a new risk or vulnerability is identified to the components or architecture of the eSourcing Service ;
       3. a change in the threat profile;
       4. a Sub-contractor failure to comply with the Service Risk Management Documentation;
       5. a significant change to any risk component;
       6. a significant change in the quantity of Personal Data held within the eSourcing Service;
       7. a proposal to change any of the Sites from which any part of the Services are provided; and/or
       8. an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns,
   16. If the Supplier fails to implement a change which is set out in the Required Changes Register by the date agreed with the Authority, such failure shall constitute a material Default and the Supplier shall:
       1. immediately cease using the Service to Process Authority Data until the Default is remedied, unless directed otherwise by the Authority in writing and then it may only continue to Process Authority Data in accordance with the Authority 's written directions; and
       2. where such Default is capable of remedy, the Supplier shall remedy such Default within the timescales set by the Authority and, should the Supplier fail to remedy the Default within such timescales, the Authority may terminate this Agreement with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 15.
   17. The Supplier shall review each Change Request against the eSourcing Risk Management Documentation to establish whether the documentation would need to be amended should such Change Request be agreed and, where a Change Request would require an amendment to the eSourcing Risk Management Documentation, the Supplier shall set out any proposed amendments to the documentation in the Impact Assessment associated with such Change Request for consideration and approval by the Authority.
   18. The Supplier shall be solely responsible for the costs associated with developing and updating the eSourcing Risk Management Documentation and carrying out any remedial action required by the Authority as part of the Accreditation process.
4. Security Assurance
   1. The Authority and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Authority’s rights under this Schedule.
   2. The Parties acknowledge that the purpose of Risk Management Documentation and associated security management processes are to ensure a good organisational approach to security under which the specific requirements of this Contract will be met.
   3. The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:
      1. [Redacted]
      2. [Redacted]
   4. The Authority has articulated its high level security outcomes in this schedule so that the Supplier can ensure that the Risk Management Documentation, security related activities and any mitigations are driven by these fundamental needs.
   5. Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.
   6. The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Government Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Government Data remains under the effective control of the Supplier at all times.
   7. The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.
   8. The Authority and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer’s security provisions represents an unacceptable risk to the Authority requiring immediate communication and co-operation between the Parties.
   9. The Statement of Information Risk Appetite and the Baseline Security Requirements shall inform the Security Assurance of the eSourcing Service. The Supplier shall provide evidence of the delivery of the security outcomes and the associated measures for each of the following:
      1. Security Risk Assessment – The Supplier shall undertake a Service specific security risk assessment
      2. Secure Design – The Supplier shall include evidence within the Risk Management Documentation on the intended approach to delivery of the security outcomes and associate measures and evidence that the associated security controls incorporate appropriate NCSC and Industry best practice.
      3. Secure Implementation – The Supplier shall undertake security testing as defined in this Schedule which evidence the service specific implementation of the measures designed to deliver the security outcomes and that security vulnerabilities have been identified and are being managed.
      4. Operational Security The Supplier shall provide evidence on an ongoing basis of the effective operations of the security controls and application of threat intelligence throughout the contract period
      5. Authority Oversight – The Authority shall be provided with regular report of the effectiveness of the security measure throughout the contracting period.
5. Risk Management Documentation
   1. The Supplier shall develop and submit to the Authority’s Approval Risk Management Documentation for the purposes of this Contract and shall comply with the requirements of Paragraphs 6.2 to 6.3.
   2. The Risk Management Documentation shall:
      1. unless otherwise specified by the Authority in writing, be developed to evidence that appropriate security controls are in place to protect all aspects of the Service and all processes associated with the provision of the Service, including the Authority Premises, the Sites, the Supplier System, the Authority System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Buyer’s Confidential Information and the Government Data) to the extent used by the Authority or the Supplier in connection with this Contract;
      2. comply with the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 5;
      3. at all times provide a level of security which:
         1. is in accordance with the Law and this Contract;
         2. complies with the Baseline Security Requirements Annex 1;
         3. as a minimum demonstrates implementation of HMG Security Guidance, Vendor recommendation and Good Industry Practice;
         4. complies with the HMG Security Policy Framework;
         5. described the implementation of security controls to deliver the eSourcing security outcomes;
         6. meets any specific security threats of immediate relevance which has been identified through a formal risk assessment of the Service, the Deliverables and/or Government Data and
      4. document the security operational procedures which shall enable the Authority to assure the ongoing management of the security controls are in place and are effective;
      5. document the vulnerability management policy including processes and security testing for identification of system vulnerabilities and assessment of the potential impact on the Deliverables of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of remediation action, testing the effectiveness of the controls,
      6. document a formal risk assessment of the Service and a risk treatment plan;
      7. the Register of Required Changes to remediate security risks
      8. addresses all security requirements as defined within this security schedule
      9. a completed Statement unless such requirement is waived by the Authority, of proposed controls for:
         1. the Service
         2. the process for managing any security risks from Sub-contractors and third parties authorised by the Authority with access to the Services, processes associated with the delivery of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System (to extent that it is under the control of the Supplier) and
         3. any IT, Information and data (including the Authority Confidential Information and the Authority Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services; and
      10. evidence that the Supplier and each applicable Sub-contractor is compliant with requirements in this Schedule.
   3. Standards, guidance and policies contained or set out in Paragraph 3.3 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.
   4. In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 6.2 the Supplier shall immediately notify the Authority representative of such inconsistency. The Authority Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.
6. Security Management Plan
   1. The Supplier shall prepare and submit to the Authority for Approval in accordance a fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph##.
   2. The Security Management Plan shall:
      1. be based on the initial Security Management Plan Template in Annex ;
      2. described how the Supplier is proposing to evidence compliance with the required security outcomes ;
      3. identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;
      4. detail the process for managing any security risks from Subcontractors and third parties authorised by the Authority with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Authority Premises, the Sites, the Supplier System, the Authority (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer’s Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on achievement of the required security outcomes;
      5. unless otherwise specified by the Authority in writing, be developed to show how evidence is to be provided that appropriate protection is in place for all aspects of the Service;
      6. States how the Supplier proposes to detail security controls to deliver the security outcomes
      7. Reference where it is proposed to evidence the delivery of this Schedule through consideration of available, appropriate and practicable pan-government accredited services;
      8. set out the plans for managing the transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the Risk Management Documentation within the timeframe agreed between the Parties;
      9. set out the scope of the Authority System that is under the control of the Supplier;
      10. be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Authority engaged in the Deliverables and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule;
      11. the dates on which each subsequent iteration of the eSourcing Risk Management Documentation will be delivered to the Authority for review and staged approval; and
      12. the date by which the Supplier is required to have received a Risk Management Approval Statement from the Authority together with details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Authority Responsibilities which must be satisfied in order for the Supplier to receive a Risk Management Approval Statement pursuant to Paragraph 4.
   3. If the Security Management Plan submitted to the Authority pursuant to Paragraph ## is Approved by the Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Authority, the Supplier shall amend it within twenty (20) Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than ten (10) Working Days from the date of the first submission to the Authority of the Security Management Plan. If the Authority does not approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Authority pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 7.2 shall be deemed to be reasonable.
   4. Approval by the Authority of the Security Management Plan pursuant to Paragraph 4 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.
7. Amendment of the Security Documentation
   1. The Risk Management Documentation and associated Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:
      1. emerging changes in Good Industry Practice;
      2. any change or proposed change to the Supplier System, the Deliverables and/or associated processes;
      3. any new perceived or changed security threats;
      4. any changes to the Security Policy;
      5. any new perceived or changed security threats; and
      6. any reasonable change in requirement requested by the Buyer.
   2. The Supplier shall provide the Authority with the results of such reviews as soon as reasonably practicable after their completion and amend the Risk Management Documentation and Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:
      1. suggested improvements to the effectiveness of the Risk Management Documentation;
      2. updates to the risk assessments;
      3. proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the Risk Management Documentation; and
      4. suggested improvements in measuring the effectiveness of controls.
   3. Subject to Paragraph 8.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 8.1, an Authority request, a change to Annex 1 (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.
   4. The Authority may, acting reasonably, Approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.
8. Certification Requirements
   1. The Supplier shall ensure, at all times during the Term, that the Supplier and any Sub-contractor with access to Authority Data or who will process Authority Data are certified as compliant with:
      1. ISO/IEC 27001:2013 by a UKAS approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and
      2. Cyber Essentials PLUS,
9. and shall provide the Authority with a copy of each such certificate of compliance before the Supplier or the relevant Sub-contractor (as applicable) shall be permitted to use the Core Information Management System to receive, store or Process any Authority Data. Any exceptions to the flow-down of the certification requirements to third party suppliers and sub-contractors must be agreed with the Authority.
   1. The Supplier shall ensure, at all times during the Term, that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data:
      1. securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and
      2. are certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the Authority.
10. The Supplier shall provide the Authority with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph before the Supplier or the relevant Sub-contractor (as applicable) shall be permitted to carry out the secure destruction of the Authority Data.
    1. The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within two (2) Working Days, if the Supplier or any Sub-contractor ceases to be compliant with the Certification Requirements and, on request from the Authority, shall ensure that the relevant Sub-contractor shall:
       1. immediately ceases processing and access to the Authority Data; and
       2. the relevant Sub-contractor promptly returns, destroys and/or erases the Authority Data in accordance with Baseline Security Requirements and Paragraph.
11. Security Testing
    1. The Supplier shall, at its own cost and expense:
       1. procure a CHECK IT Health Check of the Service (an "**IT Health Check**") by a NCSC approved member of the CHECK Scheme:
          1. prior to it submitting the eSourcing Risk Management Documentation to the Authority for an Accreditation Decision;
          2. if directed to do so by the Authority in accordance with Paragraph 10.2; and
          3. once every 12 months during the Term.
       2. conduct vulnerability scanning and assessments of the Service on a monthly basis;
       3. conduct an assessment as soon as reasonably practicable following receipt by the Supplier or any of its Sub-contractors of a critical vulnerability alert from a Supplier of any software or other component of the Service to determine whether the vulnerability affects the Service; and
       4. conduct such other tests as are required by:
          1. any Vulnerability Correction Plans;
          2. the ISO27001 certification requirements;
          3. the eSourcing Risk Management Documentation; and
          4. the Authority following a Breach of Security or a significant change to the components or architecture of the Service,
       5. (each a "**Security Test**").
    2. The Supplier shall provide the Authority with the results of such Security Tests (in a form approved by the Authority in advance) as soon as practicable after completion of each Security Test.
    3. In relation to each IT Health Check, the Supplier shall:
       1. agree with the Authority the aim and scope of the IT Health Check;
       2. promptly, following receipt of each IT Health Check report, provide the Authority with an unabridged copy of the IT Health Check report ;
       3. in the event that the IT Health Check report identifies any vulnerability, the Supplier shall:
          1. prepare a remedial plan for approval by the Authority (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the IT Health Check report:
             1. how the vulnerability will be remedied;
             2. the date by which the vulnerability will be remedied;
             3. the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Authority , include a further IT Health Check) to confirm that the vulnerability has been remedied;
          2. comply with the Vulnerability Correction Plan; and
          3. conduct such further Security Tests on the Core Information Management System as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.
    4. The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the Service) and additionally after any change or amendment to the Risk Management Documentation. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier’s ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.
    5. The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Authority with the results of such Security Tests (in a form approved by the Authority in advance) as soon as practicable after completion of each Security Test.
    6. Without prejudice to any other right of audit or access granted to the Authority pursuant to this Contract, the Authority and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the Risk Management Documentation and the Supplier's compliance with the Risk Management Documentation and the Security Management Plan. The Authority may notify the Supplier of the results of such tests after completion of each such test. If any such Authority’s test adversely affects the Supplier’s ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer’s test.
    7. Where any Security Test carried out pursuant to Paragraph 10 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Authority of any changes to the Risk Management Documentation and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Authority’s prior written Approval, the Supplier shall implement such changes to the Risk Management Documentation and repeat the relevant Security Tests in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the Risk Management Documentation is to address a residual security risk outside the Authority’s risk appetite or the requirements of this Schedule, the change to the Risk Management Documentation shall be at no cost to the Buyer.
    8. If any repeat Security Test carried out pursuant to Paragraph 10.7 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.
12. Authority auditing of Risk Management Documentation
    1. The Authority shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the Security Risk profile remains within the Authority’s Risk Appetite.
    2. If, on the basis of evidence provided by such security audits, it is the Authority’s reasonable opinion that the Service does not comply with the principles and Risk Management Documentation, then the Authority shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time then the Authority shall have the right to obtain an independent audit against these standards in whole or in part.
    3. If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practices of Risk Management Documentation then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Authority in obtaining such audit.
13. Security Incident
    1. Either Party shall notify the other in accordance with the agreed security incident management process as defined by the Risk Management Documentation upon becoming aware of any breach of security or any potential or attempted Breach of Security.
    2. Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 12.1, the Supplier shall:
       1. immediately take all reasonable steps (which shall include any action or changes reasonably required by the Authority) necessary to:
          1. minimise the extent of actual or potential harm caused by any Breach of Security;
          2. remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Authority Property and/or Authority Assets to the extent that this is within the Supplier’s control;
          3. apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier’s ability to provide the Deliverables so as to meet the relevant KPI Performance Measures, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;
          4. prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and
          5. supply any requested data to the Authority (or the Computer Emergency Response Team for UK Government) on the Buyer’s request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and
          6. as soon as reasonably practicable provide to the Authority full details (using the reporting mechanism defined by the Risk Management Documentation) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.
    3. In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Risk Management Documentation or the requirements of this Schedule, then any required change to the Risk Management Documentation shall be at no cost to the Buyer.
14. Vulnerabilities Management
    1. The Authority and the Supplier acknowledge that from time to time vulnerabilities in the eSourcing Service will be discovered which unless mitigated will present an unacceptable risk to the Authority’s information.
    2. The Supplier shall make provision for the collection of potential eSourcing service consumers’ vulnerability information arising from connecting the and for this to be made available to the Authority.
    3. The severity of vulnerabilities for the Service Providers and Third Party products used to enable the delivery of the service shall be categorised by the Supplier as ‘Critical’, ‘Important’ and ‘Other’ by aligning these categories to the vulnerability scoring according to the agreed method in the eSourcing Risk Management Documentation and using the appropriate vulnerability scoring systems including:
       1. the ‘National Vulnerability Database’ ‘Vulnerability Severity Ratings’: ‘High’, ‘Medium’ and ‘Low’ respectively (these in turn are aligned to CVSS scores as set out by NIST at http://nvd.nist.gov/cvss.cfm); and
       2. Microsoft’s ‘Security Bulletin Severity Rating System’ ratings ‘Critical’, ‘Important’, and the two remaining levels (‘Moderate’ and ‘Low’) respectively.
    4. Subject to Paragraph 13.3, the Supplier shall ensure either:
       1. the Authority agrees to tolerate vulnerability for a defined period subject to implementation of agree mitigating controls or
       2. the application of security patches to vulnerabilities in the Service within:
          1. 7 days after the public release of patches for those vulnerabilities categorised as ‘Critical’;
          2. 30 days after the public release of patches for those vulnerabilities categorised as ‘Important’; and
          3. 60 days after the public release of patches for those vulnerabilities categorised as ‘Other’.
    5. The timescales for applying patches to vulnerabilities in the eSourcing Service set out in Paragraph 13.4 shall be extended where:
       1. the Supplier can demonstrate that a vulnerability in the eSourcing Service is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the timescales set out in Paragraph 13.4 if the vulnerability becomes exploitable within the context of the Services;
       2. the application of a ‘Critical’ or ‘Important’ security patch adversely affects the Supplier’s ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or
       3. the Authority agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the eSourcing Risk Management Documentation.
15. Operational Security Management/Reporting
    1. The Service Provider shall include provisions for major version upgrades of all Supplier COTS Software and Third Party COTS Software to be upgraded within 6 Months of the release of the latest version, such that the version of the software is under mainstream vendor support throughout the Term unless:
       1. is agreed with the Authority in writing.
    2. The Supplier shall:
       1. implement a mechanism for receiving, analysing and acting upon threat information supplied by the UK CERT, or any other competent Central Government Body;
       2. ensure that the eSourcing Service is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;
       3. ensure the Supplier security personnel are knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the eSourcing service by actively monitoring the threat landscape during the Contract Period;
       4. pro-actively scan the eSourcing for vulnerable components and address discovered vulnerabilities through the processes described in the Risk Management Documentation as developed under Paragraph 6;
       5. from the date specified in the Risk Management Documentation provide a report to the Authority a monthly report provide agree evidence of the continuing effectiveness of the on-going security controls described in the Risk Management Documentation
       6. remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of eSourcing Service ); and
       7. inform the Authority when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.
    3. If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 13.4, the Supplier shall immediately notify the Buyer.
16. Off Shoring
    1. The Service Provider shall provide the Aurthority with a statement of the physical location where its data shall be stored, processed and managed. Where part or all of the Service is not delivered from:
       1. Country within the EEA
       2. Country’s where the European Commission has made a positive finding with regard to the adequacy of their regulatory Data Protection controls or;
       3. Supplier who has Privacy Shield

The Supplier shall obtain approval from the Authority for the off-shored elements.

1. Contract Termination
   1. The Supplier upon termination of the eSourcing contract shall have:
      1. On demand provide the Authority with all the eSourcing data in an agree open format
      2. Have documented process to ensure the availability of the eSourcing Data In the event the Supplier ceasing to trade;
      3. Securely erase any or all the eSourcing data held by the Supplier when requested to do so by the Authority in accordance with the Risk Management Documentation
      4. Securely destroy all media that held eSourcing data in accordance with the Risk Management Documentation

|  |  |
| --- | --- |
| **Service Security Measure** | **Description** |
| Data-in-transit protection between clients and service | The Service protects external data in transits via untrusted network between the service and client End User Devices using TLS or other appropriate protection |
| Industry good practice external certificate configuration | The Service protect external data in transit using correctly configured certificates |
| Data-in-transit protection between micro-services | The Service protect internal data in transit between services using encryption when transiting between different service providers |
| Industry good practice internal certificate configuration | The Service protect internal data in transit between services using correctly configured certificates |
| API authentication and protection | If APIs are available, the Service protects both internal and external APIs through a robust authentication method |
| Privilege separation | If there is a concept of privilege levels in the service, the Service whilst allow the ability for low privilege users to be created and for access to the service. However, this access should be restricted to only functionality that is needed to perform their business function and where the security risk is assessed as bring manageable. |
| Privilege Access Management | For User who required access to functionality which gives them pervasive access to the service then more robust security controls should be applied to this access to ensure the security risk is managed |
| Logging and event collection | The Service shall undertake appropriate logging to detect malicious action and this may include security logs and resource logs |
| Availability of logs and Alerting | The Service must make logs available to the Svc Mgmt. Team and provided appropriate alerts to inform Service Managers of potential malicious incidents. |
| Clear vulnerability response to patching and security issues | The Service shall have a clear vulnerability response and patching system in place to remedy any publicly reported issues in their service, or libraries that the service makes use of and meet the requires defined in the security schedule |
| Physical location and Legal Jurisdiction | The location of countries where the data will be stored, processed and managed. To ensure that consideration as to how this affects Service compliance with relevant legislation e.g. GDPR |
| Data Centre Security | The physical security measures employed by the provider are sufficient for your intended use of the service |
| Data at Rest Protection | Storage media containing your data are protected from unauthorised access. |
| Data Sanitisation | The data is erased when resources are moved or re-provisioned, when they leave the service or when you request it to be erased  Storage media which has held eSourcing data is sanitised or securely destroyed at the end of its life |
| Equipment disposal | All equipment potentially containing your data, credentials, or configuration information for the service is identified at the end of its life (or prior to being recycled).  Any components containing sensitive data are sanitised, removed or destroyed as appropriate  Accounts or credentials specific to redundant equipment are revoked to reduce their value to an attacker.. |
| Physical resilience and availability | The controls in place to ensure that the service meets the Business requirement for availability, including their ability to recover from outages. |
| Governance Framework | A clearly identified, and named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service. A documented framework for security governance, with policies governing key aspects of information security relevant to the service. Security and information security are part of the service provider’s financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risk. Processes to identify and ensure compliance with applicable legal and regulatory requirements. |
| Risk Assessment | To ensure that the service has pro-actively assessed the threat environment within which the service has to operate and put in place appropriate measure to manage the identified security risks. |
| Configuration and Change Management | The status, location and configuration of service components (both hardware and software) are tracked throughout their lifetime.  Changes to the service are assessed for potential security impact. Then managed and tracked through to completion. |
| Incident Management | Incident management processes are in place for the service and are actively deployed in response to security incidents. Pre-defined processes are in place for responding to common types of incident and attack. A defined process and contact route exists for reporting of security incidents by consumers and external entities. Security incidents of relevance to you will be reported in acceptable timescales and formats |
| Personnel Security | The level of security screening conducted on service provider staff with access to your information, or with ability to affect your service, is appropriate. The minimum number of people necessary have access to your information or could affect your service |
| Supply Chain Security | There are agreements defined to enable the secure information sharing with, or accessible to, third party suppliers and *their* supply chains. Any sub-contracted service used shall deliver the Service security outcomes and the procurement process places this obligation on third party suppliers. The service provider shall be able to demonstrate management of security risks arising from third party suppliers and has process in place to ensure conformance of their suppliers with security requirements. |
| Secure Service Administration | Controls shall be in place to ensure that other users cannot access, modify or otherwise affect your service management. To manage the risks of privileged access using a appropriate security controls such as the ‘principle of least privilege’. |
| Identity and authentication | The Service has controls in place to identity and authenticate users thereby ensuring only are authorised access to interface is granted. |
| External Interface Protection | The Service’ physical and logical interfaces provide appropriate protection to protect the confidentiality, availability and integrity of data and that the security risk associated with this access is managed. The security controls in place to identify and authenticates users shall be robust enough to mitigate the security risk associated with the identified interface and information being exchanged |
| Secure Design Principles | The service Design process addresses new and evolving threats are reviewed and the service improved in line with them. Development is carried out in line with NCSC good practice regarding secure design, coding, testing and deployment. Configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment. |