

# Digital Outcomes and Specialists 5 (RM1043.7)

# Call-Off Schedules

Version 2

Crown Copyright 2020

Contents

[Call-Off Schedule 1 (Transparency Reports) 3](#_Toc76636796)

[Call-Off Schedule 2 (Staff Transfer) 5](#_Toc76636799)

[Call-Off Schedule 3 (Continuous Improvement) 15](#_Toc76636809)

[Call-Off Schedule 4 (Call Off Tender) 17](#_Toc76636812)

[Call-Off Schedule 5 (Pricing Details and Expenses Policy) 19](#_Toc76636813)

[Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables) 23](#_Toc76636815)

[Call-Off Schedule 7 (Key Supplier Staff) 31](#_Toc76636826)

[Call-Off Schedule 9 (Security) 32](#_Toc76636828)

[Call-Off Schedule 10 (Exit Management) 45](#_Toc76636851)

[Call-Off Schedule 13 (Implementation Plan and Testing) 52](#_Toc76636862)

[Call-Off Schedule 17 (MOD Terms) 65](#_Toc76636892)

[Call-Off Schedule 18 (Background Checks) 69](#_Toc76636901)

[Call-Off Schedule 20 (Call-Off Specification) 71](#_Toc76636906)

[Call-Off Schedule 26 (Cyber Essentials Scheme) 108](#_Toc76636931)

## Call-Off Schedule 1 (Transparency Reports)

### Transparency Reports

* 1. The Supplier recognises that the Buyer is subject to PPN 01/17 (Updates to transparency principles v1.1 (<https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles>). The Supplier shall comply with the provisions of this Schedule in order to assist the Buyer with its compliance with its obligations under that PPN.
  2. Without prejudice to the Supplier's reporting requirements set out in the Framework Contract, within three (3) Months of the Start Date the Supplier shall submit to the Buyer for Approval (such Approval not to be unreasonably withheld or delayed) draft Transparency Reports consistent with the content requirements and format set out in the Annex of this Schedule.
  3. If the Buyer rejects any proposed Transparency Report submitted by the Supplier, the Supplier shall submit a revised version of the relevant report for further Approval within five (5) days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Buyer. If the Parties fail to agree on a draft Transparency Report the Buyer shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.
  4. The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Buyer at the frequency referred to in the Annex of this Schedule.

### Annex A: List of Transparency Reports

|  |  |  |
| --- | --- | --- |
| **Title** | **Content** | **Frequency** |
| **Performance metrics** | Progress Report | Monthly |
| **Call-Off Contract Charges** | Contract Value | As updated |
| **Key Subcontractors and supply chain governance** | List of key Subcontractors and supply chain governance processes | As required |
| **Performance and underperformance management** | Service Improvement Plan | As required |
| **Resource plans** | Resource Plan including Key Personnel Management | As required |

## Call-Off Schedule 2 (Staff Transfer)

### Definitions

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

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Employee Liability** | all claims, actions, proceedings, orders, demands, complaints, investigations (save for any claims for personal injury which are covered by insurance) and any award, compensation, damages, tribunal awards, fine, loss, order, penalty, disbursement, payment made by way of settlement and costs, expenses and legal costs reasonably incurred in connection with a claim or investigation including in relation to the following:   1. redundancy payments including contractual or enhanced redundancy costs, termination costs and notice payments; 2. unfair, wrongful or constructive dismissal compensation; 3. compensation for discrimination on grounds of sex, race, disability, age, religion or belief, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation or claims for equal pay; 4. compensation for less favourable treatment of part-time workers or fixed term employees; 5. outstanding debts and unlawful deduction of wages including any PAYE and National Insurance Contributions in relation to payments made by the Buyer or the Replacement Supplier to a Transferring Supplier Employee which would have been payable by the Supplier or the Subcontractor if such payment should have been made prior to the Service Transfer Date and also including any payments arising in respect of pensions; 6. claims whether in tort, contract or statute or otherwise;   any investigation by the Equality and Human Rights Commission or other enforcement, regulatory or supervisory body and of implementing any requirements which may arise from such investigation; |
| **Former Supplier** | a supplier supplying the Deliverables to the Buyer before the Relevant Transfer Date that are the same as or substantially similar to the Deliverables (or any Part of the Deliverables) and shall include any Subcontractor of such supplier (or any Subcontractor of any such Subcontractor); |
| **Partial Termination** | the partial termination of the relevant Contract to the extent that it relates to the provision of any Part of the Services as further provided for in Clause 10.4 (When CCS or the Buyer can end this contract) or 10.6 (When the Supplier can end the contract); |
| **Relevant Transfer** | a transfer of employment to which the Employment Regulations applies; |
| **Relevant Transfer Date** | in relation to a Relevant Transfer, the date upon which the Relevant Transfer takes place, and for the purposes of Part D: Pensions, shall include the Commencement Date, where appropriate; |
| **Supplier's Final Supplier Personnel List** | a list provided by the Supplier of all Supplier Personnel whose will transfer under the Employment Regulations on the Service Transfer Date; |
| **Supplier's Provisional Supplier Personnel List** | a list prepared and updated by the Supplier of all Supplier Personnel who are at the date of the list wholly or mainly engaged in or assigned to the provision of the Services or any relevant Part of the Services which it is envisaged as at the date of such list will no longer be provided by the Supplier; |
| **Staffing Information** | in relation to all persons identified on the Supplier's Provisional Supplier Personnel List or Supplier's Final Supplier Personnel List, as the case may be, such information as the Buyer may reasonably request (subject to all applicable provisions of the Data Protection Laws), but including in an anonymised format:   1. their ages, dates of commencement of employment or engagement, gender and place of work; 2. details of whether they are employed, self-employed contractors or consultants, agency workers or otherwise; 3. the identity of the employer or relevant contracting Party; 4. their relevant contractual notice periods and any other terms relating to termination of employment, including redundancy procedures, and redundancy payments; 5. their wages, salaries, bonuses and profit sharing arrangements as applicable; 6. details of other employment-related benefits, including (without limitation) medical insurance, life assurance, pension or other retirement benefit schemes, share option schemes and company car schedules applicable to them; 7. any outstanding or potential contractual, statutory or other liabilities in respect of such individuals (including in respect of personal injury claims); 8. details of any such individuals on long term sickness absence, parental leave, maternity leave or other authorised long term absence; 9. copies of all relevant documents and materials relating to such information, including copies of relevant contracts of employment (or relevant standard contracts if applied generally in respect of such employees); and 10. any other "employee liability information" as such term is defined in regulation 11 of the Employment Regulations; |
| **Term** | the period commencing on the Start Date and ending on the expiry of the Initial Period or any Extension Period or on earlier termination of the relevant Contract; |
| **Transferring Buyer Employees** | those employees of the Buyer to whom the Employment Regulations will apply on the Relevant Transfer Date and whose names are provided to the Supplier on or prior to the Relevant Transfer Date; and |
| **Transferring Former Supplier Employees** | in relation to a Former Supplier, those employees of the Former Supplier to whom the Employment Regulations will apply on the Relevant Transfer Date and whose names are provided to the Supplier on or prior to the Relevant Transfer Date. |

### Interpretation

Where a provision in this Schedule imposes any obligation on the Supplier including (without limit) to comply with a requirement or provide an indemnity, undertaking or warranty, the Supplier shall procure that each of its Subcontractors shall comply with such obligation and provide such indemnity, undertaking or warranty to CCS, the Buyer, Former Supplier, Replacement Supplier or Replacement Subcontractor, as the case may be and where the Subcontractor fails to satisfy any claims under such indemnities the Supplier will be liable for satisfying any such claim as if it had provided the indemnity itself.

### Which parts of this Schedule apply

Only the:

* 1. parts of this Schedule identified in the Order Form shall apply to this Call-Off Contract; or
  2. following parts of this Schedule shall apply to this Call-Off Contract:
* Part C (No Staff Transfer On Start Date)
* Part E (Staff Transfer on Exit)

### Part C: No Staff Transfer on the Start Date

### What happens if there is a staff transfer

* 1. The Buyer and the Supplier agree that the commencement of the provision of the Services or of any Part of the Services will not be a Relevant Transfer in relation to any employees of the Buyer and/or any Former Supplier.
  2. Subject to Paragraphs 1.3, 1.4 and 1.5, if any employee of the Buyer and/or a Former Supplier claims, or it is determined in relation to any employee of the Buyer and/or a Former Supplier, that his/her contract of employment has been transferred from the Buyer and/or the Former Supplier to the Supplier and/or any Subcontractor pursuant to the Employment Regulations then:
     1. the Supplier will, within 5 Working Days of becoming aware of that fact, notify the Buyer in writing;
     2. the Buyer may offer employment to such person, or take such other steps as it considered appropriate to resolve the matter, within 10 Working Days of receipt of notice from the Supplier;
     3. if such offer of employment is accepted, the Supplier shall immediately release the person from its employment;
     4. if after the period referred to in paragraph 1.2.2 no such offer has been made, or such offer has been made but not accepted, the Supplier may within 5 Working Days give notice to terminate the employment of such person;

and subject to the Supplier's compliance with Paragraphs 1.2.1 to 1.2.4:

1. the Buyer will indemnify the Supplier and/or the relevant Subcontractor against all Employee Liabilities arising out of the termination of the employment of any of the Buyer's employees referred to in Paragraph 1.2; and
2. the Buyer will procure that the Former Supplier indemnifies the Supplier and/or any Subcontractor against all Employee Liabilities arising out of termination of the employment of the employees of the Former Supplier referred to in Paragraph 1.2.
   1. The indemnities in Paragraph 1.2 shall not apply to any claim:
      1. for discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief or equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees in relation to any alleged act or omission of the Supplier and/or Subcontractor; or
      2. any claim that the termination of employment was unfair because the Supplier and/or any Subcontractor neglected to follow a fair dismissal procedure
   2. The indemnities in Paragraph 1.2 shall not apply to any termination of employment occurring later than 3 Months from the Commencement Date.
   3. If the Supplier and/or the Subcontractor does not comply with Paragraph 1.2, all Employee Liabilities in relation to such employees shall remain with the Supplier and/or the Subcontractor and the Supplier shall (i) comply with the provisions of Part D: Pensions of this Schedule, and (ii) indemnify the Buyer and any Former Supplier against any Employee Liabilities that either of them may incur in respect of any such employees of the Supplier and/or employees of the Subcontractor.

### Limits on the Former Supplier’s obligations

Where in this Part C the Buyer accepts an obligation to procure that a Former Supplier does or does not do something, such obligation shall be limited so that it extends only to the extent that the Buyer's contract with the Former Supplier contains a contractual right in that regard which the Buyer may enforce, or otherwise so that it requires only that the Buyer must use reasonable endeavours to procure that the Former Supplier does or does not act accordingly.

### Part E: Staff Transfer on Exit

Obligations before a Staff Transfer

### Obligations before a Staff Transfer

* 1. The Supplier agrees that within 20 Working Days of the earliest of:
     1. receipt of a notification from the Buyer of a Service Transfer or intended Service Transfer;
     2. receipt of the giving of notice of early termination or any Partial Termination of the relevant Contract;
     3. the date which is 12 Months before the end of the Term; and
     4. receipt of a written request of the Buyer at any time (provided that the Buyer shall only be entitled to make one such request in any 6 Month period),

it shall provide in a suitably anonymised format so as to comply with the Data Protection Laws, the Supplier's Provisional Supplier Personnel List, together with the Staffing Information in relation to the Supplier's Provisional Supplier Personnel List and it shall provide an updated Supplier's Provisional Supplier Personnel List at such intervals as are reasonably requested by the Buyer.

* 1. At least 20 Working Days prior to the Service Transfer Date, the Supplier shall provide to the Buyer or at the direction of the Buyer to any Replacement Supplier and/or any Replacement Subcontractor (i) the Supplier's Final Supplier Personnel List, which shall identify the basis upon which they are Transferring Supplier Employees and (ii) the Staffing Information in relation to the Supplier’s Final Supplier Personnel List (insofar as such information has not previously been provided).
  2. The Buyer shall be permitted to use and disclose information provided by the Supplier under paragraphs 1.1 and 1.2 for the purpose of informing any prospective Replacement Supplier and/or Replacement Subcontractor.
  3. The Supplier warrants, for the benefit of The Buyer, any Replacement Supplier, and any Replacement Subcontractor that all information provided pursuant to paragraphs 1.1 and 1.2 shall be true and accurate in all material respects at the time of providing the information.
  4. From the date of the earliest event referred to in Paragraph 1.1.1, 1.1.2 and 1.1.3, the Supplier agrees that it shall not assign any person to the provision of the Services who is not listed on the Supplier’s Provisional Supplier Personnel List and shall, unless otherwise instructed by the Buyer (acting reasonably):
     1. not replace or re-deploy any Supplier Personnel listed on the Supplier Provisional Supplier Personnel List other than where any replacement is of equivalent grade, skills, experience and expertise and is employed on the same terms and conditions of employment as the person he/she replaces
     2. make, promise, propose, permit or implement any material changes to the terms and conditions of (i) employment and/or (ii) pensions, retirement and death benefits (including not to make pensionable any category of earnings which were not previously pensionable or reduce the pension contributions payable) of the Supplier Personnel (including any payments connected with the termination of employment);
     3. not increase the proportion of working time spent on the Services (or the relevant Part of the Services) by any of the Supplier Personnel save for fulfilling assignments and projects previously scheduled and agreed;
     4. not introduce any new contractual or customary practice concerning the making of any lump sum payment on the termination of employment of any employees listed on the Supplier's Provisional Supplier Personnel List;
     5. not increase or reduce the total number of employees so engaged, or deploy any other person to perform the Services (or the relevant Part of the Services);
     6. not terminate or give notice to terminate the employment or contracts of any persons on the Supplier's Provisional Supplier Personnel List save by due disciplinary process;
     7. not dissuade or discourage any employees engaged in the provision of the Services from transferring their employment to the Buyer and/or the Replacement Supplier and/or Replacement Subcontractor;
     8. give the Buyer and/or the Replacement Supplier and/or Replacement Subcontractor reasonable access to Supplier Personnel and/or their consultation representatives to inform them of the intended transfer and consult any measures envisaged by the Buyer, Replacement Supplier and/or Replacement Subcontractor in respect of persons expected to be Transferring Supplier Employees;
     9. co-operate with the Buyer and the Replacement Supplier to ensure an effective consultation process and smooth transfer in respect of Transferring Supplier Employees in line with good employee relations and the effective continuity of the Services, and to allow for participation in any pension arrangements to be put in place to comply with New Fair Deal;
     10. promptly notify the Buyer or, at the direction of the Buyer, any Replacement Supplier and any Replacement Subcontractor of any notice to terminate employment given by the Supplier or received from any persons listed on the Supplier's Provisional Supplier Personnel List regardless of when such notice takes effect;
     11. not for a period of 12 Months from the Service Transfer Date re-employ or re-engage or entice any employees, suppliers or Subcontractors whose employment or engagement is transferred to the Buyer and/or the Replacement Supplier (unless otherwise instructed by the Buyer (acting reasonably));
     12. not to adversely affect pension rights accrued by all and any Fair Deal Employees in the period ending on the Service Transfer Date;
     13. fully fund any Broadly Comparable pension schemes set up by the Supplier;
     14. maintain such documents and information as will be reasonably required to manage the pension aspects of any onward transfer of any person engaged or employed by the Supplier or any Subcontractor in the provision of the Services on the expiry or termination of this Contract (including without limitation identification of the Fair Deal Employees);
     15. promptly provide to the Buyer such documents and information mentioned in Paragraph 3.1.1 of Part D: Pensions which the Buyer may reasonably request in advance of the expiry or termination of this Contract; and
     16. fully co-operate (and procure that the trustees of any Broadly Comparable pension scheme shall fully co-operate) with the reasonable requests of the Supplier relating to any administrative tasks necessary to deal with the pension aspects of any onward transfer of any person engaged or employed by the Supplier or any Subcontractor in the provision of the Services on the expiry or termination of this Contract.
  5. On or around each anniversary of the Effective Date and up to four times during the last 12 Months of the Term, the Buyer may make written requests to the Supplier for information relating to the manner in which the Services are organised. Within 20 Working Days of receipt of a written request the Supplier shall provide such information as the Buyer may reasonably require which shall include:
     1. the numbers of employees engaged in providing the Services;
     2. the percentage of time spent by each employee engaged in providing the Services;
     3. the extent to which each employee qualifies for membership of any of the Fair Deal Schemes (as defined in Part D: Pensions); and
     4. a description of the nature of the work undertaken by each employee by location.
  6. The Supplier shall provide all reasonable cooperation and assistance to the Buyer, any Replacement Supplier and/or any Replacement Subcontractor to ensure the smooth transfer of the Transferring Supplier Employees on the Service Transfer Date including providing sufficient information in advance of the Service Transfer Date to ensure that all necessary payroll arrangements can be made to enable the Transferring Supplier Employees to be paid as appropriate. Without prejudice to the generality of the foregoing, within 5 Working Days following the Service Transfer Date, the Supplier shall provide to the Buyer or, at the direction of the Buyer, to any Replacement Supplier and/or any Replacement Subcontractor (as appropriate), in respect of each person on the Supplier's Final Supplier Personnel List who is a Transferring Supplier Employee:
     1. the most recent month's copy pay slip data;
     2. details of cumulative pay for tax and pension purposes;
     3. details of cumulative tax paid;
     4. tax code;
     5. details of any voluntary deductions from pay; and
     6. bank/building society account details for payroll purposes.

### Staff Transfer when the contract ends

* 1. A change in the identity of the supplier of the Services (or Part of the Services), howsoever arising, may constitute a Relevant Transfer to which the Employment Regulations will apply.
  2. The Buyer and the Supplier agree that where a Relevant Transfer occurs, the contracts of employment between the Supplier and the Transferring Supplier Employees (except in relation to any contract terms disapplied through operation of regulation 10(2) of the Employment Regulations) will have effect on and from the Service Transfer Date as if originally made between the Replacement Supplier and/or a Replacement Subcontractor (as the case may be) and each such Transferring Supplier Employee.
  3. The Supplier shall comply with all its obligations in respect of the Transferring Supplier Employees arising under the Employment Regulations in respect of the period up to (and including) the Service Transfer Date including (without limit) the payment of all remuneration, benefits, entitlements, PAYE, national insurance contributions and pension contributions and all such sums due as a result of any Fair Deal Employees' participation in the Fair Deal Schemes (as defined in Part D: Pensions).
  4. Subject to Paragraph 2.4, the Supplier shall indemnify the Buyer and/or the Replacement Supplier and/or any Replacement Subcontractor against any Employee Liabilities arising from or as a result of any act or omission of the Supplier or any Subcontractor in respect of any Transferring Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Supplier Employee whether occurring before, on or after the Service Transfer Date.
  5. The indemnity in paragraph 2.3 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Replacement Supplier and/or any Replacement Subcontractor whether occurring or having its origin before, on or after the Service Transfer Date.
  6. Subject to Paragraphs 2.6 and 2.7, if any employee of the Supplier who is not identified in the Supplier's Final Transferring Supplier Employee List claims, or it is determined in relation to any employees of the Supplier, that his/her contract of employment has been transferred from the Supplier to the Replacement Supplier and/or Replacement Subcontractor pursuant to the Employment Regulations then.
     1. the Replacement Supplier and/or Replacement Subcontractor will, within 5 Working Days of becoming aware of that fact, notify the Buyer and the Supplier in writing;
     2. the Supplier may offer employment to such person, or take such other steps as it considered appropriate to resolve the matter, within 10 Working Days of receipt of notice from the Replacement Supplier and/or Replacement Subcontractor;
     3. if such offer of employment is accepted, the Replacement Supplier and/or Replacement Subcontractor shall immediately release the person from its employment;
     4. if after the period referred to in Paragraph 2.5.2 no such offer has been made, or such offer has been made but not accepted, the Replacement Supplier and/or Replacement Subcontractor may within 5 Working Days give notice to terminate the employment of such person;

and subject to the Replacement Supplier's and/or Replacement Subcontractor's compliance with Paragraphs 2.5.1 to 2.5.4 the Supplier will indemnify the Replacement Supplier and/or Replacement Subcontractor against all Employee Liabilities arising out of the termination of the employment of any of the Supplier's employees referred to in Paragraph 2.5.

* 1. The indemnity in Paragraph 2.5 shall not apply to:
     1. any claim for discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief, or equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees, arising as a result of any alleged act or omission of the Replacement Supplier and/or Replacement Subcontractor, or
     2. any claim that the termination of employment was unfair because the Replacement Supplier and/or Replacement Subcontractor neglected to follow a fair dismissal procedure.
  2. The indemnity in Paragraph 2.5 shall not apply to any termination of employment occurring later than 3 Months from the Service Transfer Date.
  3. If at any point the Replacement Supplier and/or Replacement Sub-contract accepts the employment of any such person as is described in Paragraph 2.5, such person shall be treated as a Transferring Supplier Employee and Paragraph 2.5 shall cease to apply to such person.
  4. The Supplier shall promptly provide the Buyer and any Replacement Supplier and/or Replacement Subcontractor, in writing such information as is necessary to enable the Buyer, the Replacement Supplier and/or Replacement Subcontractor to carry out their respective duties under regulation 13 of the Employment Regulations. The Buyer shall procure that the Replacement Supplier and/or Replacement Subcontractor, shall promptly provide to the Supplier and each Subcontractor in writing such information as is necessary to enable the Supplier and each Subcontractor to carry out their respective duties under regulation 13 of the Employment Regulations.
  5. Subject to Paragraph 2.9, the Buyer shall procure that the Replacement Supplier indemnifies the Supplier on its own behalf and on behalf of any Replacement Subcontractor and its Subcontractors against any Employee Liabilities arising from or as a result of any act or omission, whether occurring before, on or after the Service Transfer Date, of the Replacement Supplier and/or Replacement Subcontractor in respect of any Transferring Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any such Transferring Supplier Employee.
  6. The indemnity in Paragraph 2.10 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Supplier and/or any Sub-contractor (as applicable) whether occurring or having its origin before, on or after the Service Transfer Date, including any Employee Liabilities arising from the failure by the Supplier and/or any Subcontractor (as applicable) to comply with its obligations under the Employment Regulations, or to the extent the Employee Liabilities arise out of the termination of employment of any person who is not identified in the Supplier’s Final Supplier Personnel List in accordance with Paragraph 2.5 (and subject to the limitations set out in Paragraphs 2.6 and 2.7 above).

## Call-Off Schedule 3 (Continuous Improvement)

### Buyer’s Rights

* 1. The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), the Buyer may give CCS the right to enforce the Buyer's rights under this Schedule.

### Supplier’s Obligations

* 1. The Supplier must, throughout the Contract Period, identify new or potential improvements to the provision of the Deliverables with a view to reducing the Buyer’s costs (including the Charges) and/or improving the quality and efficiency of the Deliverables and their supply to the Buyer.
  2. The Supplier must adopt a policy of continuous improvement in relation to the Deliverables, which must include regular reviews with the Buyer of the Deliverables and the way it provides them, with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables. The Supplier and the Buyer must provide each other with any information relevant to meeting this objective.
  3. In addition to Paragraph 2.1, the Supplier shall produce at the start of each Contract Year a plan for improving the provision of Deliverables and/or reducing the Charges (without adversely affecting the performance of this Contract) during that Contract Year (**"Continuous Improvement Plan"**) for the Buyer's Approval. The Continuous Improvement Plan must include, as a minimum, proposals:
     1. identifying the emergence of relevant new and evolving technologies;
     2. changes in business processes of the Supplier or the Buyer and ways of working that would provide cost savings and/or enhanced benefits to the Buyer (such as methods of interaction, supply chain efficiencies, reduction in energy consumption and methods of sale);
     3. new or potential improvements to the provision of the Deliverables including the quality, responsiveness, procedures, benchmarking methods, likely performance mechanisms and customer support services in relation to the Deliverables; and
     4. measuring and reducing the sustainability impacts of the Supplier's operations and supply-chains relating to the Deliverables, and identifying opportunities to assist the Buyer in meeting their sustainability objectives.
  4. The initial Continuous Improvement Plan for the first (1st) Contract Year shall be submitted by the Supplier to the Buyer for Approval within one hundred (100) Working Days of the first Order or six (6) Months following the Start Date, whichever is earlier.
  5. The Buyer shall notify the Supplier of its Approval or rejection of the proposed Continuous Improvement Plan or any updates to it within twenty (20) Working Days of receipt. If it is rejected then the Supplier shall, within ten (10) Working Days of receipt of notice of rejection, submit a revised Continuous Improvement Plan reflecting the changes required. Once Approved, it becomes the Continuous Improvement Plan for the purposes of this Contract.
  6. The Supplier must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Supplier shall provide any further information as requested.
  7. If the Buyer wishes to incorporate any improvement into this Contract, it must request a Variation in accordance with the Variation Procedure and the Supplier must implement such Variation at no additional cost to the Buyer or CCS.
  8. Once the first Continuous Improvement Plan has been Approved in accordance with Paragraph 2.5:
     1. the Supplier shall use all reasonable endeavours to implement any agreed deliverables in accordance with the Continuous Improvement Plan; and
     2. the Parties agree to meet as soon as reasonably possible following the start of each quarter (or as otherwise agreed between the Parties) to review the Supplier's progress against the Continuous Improvement Plan.
  9. The Supplier shall update the Continuous Improvement Plan as and when required but at least once every Contract Year (after the first (1st) Contract Year) in accordance with the procedure and timescales set out in Paragraph 2.3.
  10. All costs relating to the compilation or updating of the Continuous Improvement Plan and the costs arising from any improvement made pursuant to it and the costs of implementing any improvement, shall have no effect on and are included in the Charges.
  11. Should the Supplier's costs in providing the Deliverables to the Buyer be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Buyer by way of a consequential and immediate reduction in the Charges for the Deliverables.
  12. At any time during the Contract Period of the Call-Off Contract, the Supplier may make a proposal for gainshare. If the Buyer deems gainshare to be applicable then the Supplier shall update the Continuous Improvement Plan so as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio.

## Call-Off Schedule 4 (Call Off Tender)

Ref A: 20210519-DSA D&IP – Proposal – Rowden Technologies – V1.pdf

Ref B: 20210519-DSA D&IP – Cultural Fit – Rowden Technologies – V1.pdf

Ref C: 20210519-DSA D&IP – Pricing – Rowden Technologies – V1.pdf

Ref D: 20210615-Rowden\_Technologies\_DSA\_DIP\_Presentation\_V1.pptx

## Call-Off Schedule 5 (Pricing Details and Expenses Policy)

Call-Off Contract Charges

* 1. The Supplier shall provide:
     1. as part of the Further Competition Procedure, its pricing for the Deliverables in accordance with the Buyer’s Statement of Requirements.
     2. for each individual Statement of Work (SOW), the applicable Charges, calculated in accordance with the charging methods detailed in the Order Form and using all of the following:

1. the agreed rates for Supplier Staff and/or facilities (which are exclusive of any applicable expenses and VAT) incorporated into the Call-Off Contract;
2. the number of Work Days, or pro rata for every part of a Work Day (see Paragraph 1.2 of Framework Schedule 3 (Framework Pricing)), that Supplier Staff and/or facilities will be required to provide the Deliverables and to meet the tasks sets out in the SOW between the SOW Start Date and SOW End Date; and
3. except in the case of Lot 3 (User Research Studios), a contingency margin of up to 20% of the SOW value (“**Contingency** **Margin**”) applied to the sum calculated on the basis of (a) and (b), to accommodate any changes to the SOW Deliverables during the SOW Start Date and SOW End Date. The Supplier must (i) explain the reasons for its proposed use of, and (ii) obtain the Buyer’s Approval before applying, any amount of the Contingency Margin.
   1. Further to Paragraph 1.5 of Framework Schedule 3 (Framework Pricing), the Supplier will provide a detailed breakdown of its Charges for the Deliverables in sufficient detail to enable the Buyer to verify the accuracy of any invoice submitted.

This detailed breakdown will be incorporated into each SOW and include (but will not be limited to):

* a role description of each member of the Supplier Staff;
* a facilities description (if applicable);
* the agreed day rate for each Supplier Staff;
* any expenses charged for each Work Day for each Supplier Staff, which must be in accordance with the Buyer’s expenses policy (if applicable);
* the number of Work Days, or pro rata for every part day, they will be actively be engaged in providing the Deliverables between the SOW Start Date and SOW End Date; and
* the total SOW cost for all Supplier Staff role and facilities in providing the Deliverables.
  1. If a Capped or Fixed Price has been agreed for a particular SOW:
* the Supplier shall continue to work on the Deliverables until they are satisfactorily complete and accepted by the Buyer at its own cost and expense where the Capped or Fixed Price is exceeded; and
* the Buyer will have no obligation or liability to pay any additional Charges or cost of any part of the Deliverables yet to be completed and/or Delivered after the Capped or Fixed Price is exceeded by the Supplier.
  1. All risks or contingencies will be included in the Charges.
  2. For all additional tasks and variations, the following rates card and role descriptions shall apply:

|  |  |
| --- | --- |
| **Role** | **Role Description** |
| Business analyst | Analyse a service or organisation’s business processes and systems. Specify, collect and present findings. |
| Cyber security consultant | Minimise the chance of data or information systems security breaches. Ensure information is protected against unauthorised or unintended access. Put systems in place to prevent data destruction or disruption. |
| Data architect | Set the vision for the organisation’s use of data, through data design, to meet business needs. |
| Data engineer | Design, build, test and maintain data management systems, making sure they meet business requirements and user needs. |
| Data scientist | Identify complex business problems while working with policy and operations teams to understand where data can add value. |
| Delivery manager | Set up a team for successful delivery. Remove obstacles, track progress, facilitate meetings and help the team organise itself. |
| Designer | Provide user-centred interaction design, service design and graphic design expertise. |
| Developer | Build software that supports user needs. Continually improve the service by identifying new tools and techniques, removing technical bottlenecks, and adapting and maintaining code. |
| Performance analyst | Specify, collect and present the key performance data and analysis for a service. |
| Product manager | Lead the delivery and continuous improvement of one or more digital products or platforms. |
| Quality assurance analyst | Ensure the quality of the digital service by testing it manually and writing automated tests covering a range of conditions. |
| Service manager | Develop and deliver an effective user-focused digital service. Manage the full product lifecycle, including user research, design, delivery and continuous improvement. |
| Technical architect | Break down complex problems and identify steps towards solutions. Coach individuals and engage with non-technical people at all levels of seniority. Write code as a senior member of the development team. |
| Contract manager | Manage and process additional ad-hoc tasks. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Day Rate Card Price** | | | |
| Role | Grade | | |
| Junior (Less than 3 years’ experience in this field) | Mid (3-10 years’ experience in this field) | Senior (Over 10 years’ experience in this field) |
| Business analyst | [REDACTED] | [REDACTED] | [REDACTED] |
| Cyber security consultant | [REDACTED] | [REDACTED] | [REDACTED] |
| Data architect | [REDACTED] | [REDACTED] | [REDACTED] |
| Data engineer | [REDACTED] | [REDACTED] | [REDACTED] |
| Data scientist | [REDACTED] | [REDACTED] | [REDACTED] |
| Delivery manager | [REDACTED] | [REDACTED] | [REDACTED] |
| Designer | [REDACTED] | [REDACTED] | [REDACTED] |
| Developer | [REDACTED] | [REDACTED] | [REDACTED] |
| Performance analyst | [REDACTED] | [REDACTED] | [REDACTED] |
| Product manager | [REDACTED] | [REDACTED] | [REDACTED] |
| Quality assurance analyst | [REDACTED] | [REDACTED] | [REDACTED] |
| Service manager | [REDACTED] | [REDACTED] | [REDACTED] |
| Technical architect | [REDACTED] | [REDACTED] | [REDACTED] |
| Contract manager | [REDACTED] | [REDACTED] | [REDACTED] |

* 1. The Parties agree that the following assumptions, representations, risks and contingencies will apply in relation to the additional tasks rates card:

A working day is 8 hours, exclusive of travel and lunch.

A working week is Monday to Friday excluding national holidays.

Office hours are 09:00-17:00 Monday to Friday

The day rate prices provided shall be fixed for the duration of the contract (including the six-month extension option period).

### Annex 1 (Expenses Policy)

* + - 1. Claims for travel and subsistence can only be submitted for additional taskings and shall be in accordance with the actual limits listed in the Ministry of Defence Statement of Civilian Personnel Policy as amended from time to time.
      2. For the avoidance of doubt, any claims under this Annex 1 (Expenses Policy) shall not include any handling charges or Contractor’s profit or have VAT charged more than once.
      3. The Authority will pay claims for travel and subsistence made in accordance with this Annex 1 (Expenses Policy) up to an agreed expenses cap which is to be accepted in the additional tasking form.
      4. The Contractor shall not be entitled to claim for travel and subsistence arising out of or in connection with travel to or from and/or attendance at the following locations:
         1. Abbey Wood and/or the JPO facility;
         2. Corsham; and/or
         3. Army HQ – Andover.

## Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables)

### Definitions

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

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Buyer Property** | the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Contract; |
| **Buyer Software** | any software which is owned by or licensed to the Buyer and which is or will be used by the Supplier for the purposes of providing the Deliverables; |
| **Buyer System** | the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables; |
| **Commercial off the shelf Software or COTS Software** | Non-customised software where the IPR may be owned and licensed either by the Supplier or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms; |
| **Defect** | any of the following:   1. any error, damage or defect in the manufacturing of a Deliverable; or 2. any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or 3. any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Call Off Contract; or 4. any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Contract; |
| **Emergency Maintenance** | ad hoc and unplanned maintenance provided by the Supplier where either Party reasonably suspects that the ICT Environment or the Services, or any part of the ICT Environment or the Services, has or may have developed a fault; |
| **ICT Environment** | the Buyer System and the Supplier System; |
| **Licensed Software** | all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Call Off Contract, including any COTS Software; |
| **Maintenance Schedule** | has the meaning given to it in paragraph 8 of this Schedule; |
| **Malicious Software** | any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence; |
| **New Release** | an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item; |
| **Open Source Software** | computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge; |
| **Operating Environment** | means the Buyer System and any premises (including the Buyer Premises, the Supplier’s premises or third party premises) from, to or at which:   1. the Deliverables are (or are to be) provided; or 2. the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or 3. where any part of the Supplier System is situated; |
| **Permitted Maintenance** | has the meaning given to it in paragraph 8.2 of this Schedule; |
| **Quality Plans** | has the meaning given to it in paragraph 6.1 of this Schedule; |
| **Sites** | has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place; |
| **Software** | Specially Written Software COTS Software and non-COTS Supplier and third party Software; |
| **Software Supporting Materials** | has the meaning given to it in paragraph 9.1 of this Schedule; |
| **Source Code** | computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software; |
| **Specially Written Software** | any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR; and |
| **Supplier System** | the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System). |

### When this Schedule should be used

* 1. This Schedule is designed to provide additional provisions on Intellectual Property Rights for the Digital Deliverables.

### Buyer due diligence requirements

* 1. The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;
     1. suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Start Date) future Operating Environment;
     2. operating processes and procedures and the working methods of the Buyer;
     3. ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and
     4. existing contracts (including any licences, support, maintenance and other contracts relating to the Operating Environment) referred to in the Due Diligence Information which may be novated to, assigned to or managed by the Supplier under this Contract and/or which the Supplier will require the benefit of for the provision of the Deliverables.
  2. The Supplier confirms that it has advised the Buyer in writing of:
     1. each aspect, if any, of the Operating Environment that is not suitable for the provision of the ICT Services;
     2. the actions needed to remedy each such unsuitable aspect; and
     3. a timetable for and the costs of those actions.
  3. The Supplier undertakes:
     1. and represents to the Buyer that Deliverables will meet the Buyer’s acceptance criteria as set out in each Statement of Work; and
     2. to maintain all interface and interoperability between third party software or services, and Specially Written Software required for the performance or supply of the Deliverables.

### Licensed software warranty

* 1. The Supplier represents and warrants that:
     1. it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Sub-Contractor) to the Buyer which are necessary for the performance of the Supplier’s obligations under this Contract including the receipt of the Deliverables by the Buyer;
     2. all components of the Specially Written Software shall:
        1. be free from material design and programming errors;
        2. perform in all material respects in accordance with the relevant specifications contained in Call Off Schedule 14 (Service Levels) and Documentation; and
        3. not infringe any IPR.

### Provision of ICT Services

* 1. The Supplier shall:
     1. ensure that the release of any new COTS Software in which the Supplier owns the IPR, or upgrade to any Software in which the Supplier owns the IPR complies with the interface requirements of the Buyer and (except in relation to new Software or upgrades which are released to address Malicious Software) shall notify the Buyer three (3) Months before the release of any new COTS Software or Upgrade;
     2. ensure that all Software including upgrades, updates and New Releases used by or on behalf of the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;
     3. ensure that the Supplier System will be free of all encumbrances;
     4. ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Contract;
     5. minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables.

### Standards and Quality Requirements

* 1. The Supplier shall develop, in the timescales specified in the Order Form, quality plans that ensure that all aspects of the Deliverables are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it (**"Quality Plans"**).
  2. The Supplier shall seek Approval from the Buyer (not be unreasonably withheld or delayed) of the Quality Plans before implementing them. Approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Deliverables are provided to the standard required by this Contract.
  3. Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.
  4. The Supplier shall ensure that the Supplier Personnel shall at all times during the Call Off Contract Period:
     1. be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Contract;
     2. apply all due skill, care, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of the Deliverables; and
     3. obey all lawful instructions and reasonable directions of the Buyer (including, if so required by the Buyer, the ICT Policy) and provide the Deliverables to the reasonable satisfaction of the Buyer.

### ICT Audit

* 1. The Supplier shall allow any auditor access to the Supplier premises to:
     1. inspect the ICT Environment and the wider service delivery environment (or any part of them);
     2. review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;
     3. review the Supplier’s quality management systems including all relevant Quality Plans.

### Maintenance of the ICT Environment

* 1. If specified by the Buyer in the Order Form, the Supplier shall create and maintain a rolling schedule of planned maintenance to the ICT Environment (**"Maintenance Schedule"**) and make it available to the Buyer for Approval in accordance with the timetable and instructions specified by the Buyer.
  2. Once the Maintenance Schedule has been Approved, the Supplier shall only undertake such planned maintenance (which shall be known as **"Permitted Maintenance"**) in accordance with the Maintenance Schedule.
  3. The Supplier shall give as much notice as is reasonably practicable to the Buyer prior to carrying out any Emergency Maintenance.
  4. The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the ICT Environment and/or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the ICT Environment and the provision of the Deliverables.

### Intellectual Property Rights

* 1. **Assignments granted by the Supplier: Specially Written Software** 
     1. The Supplier assigns (by present assignment of future rights to take effect immediately on it coming into existence) to the Buyer with full guarantee (or shall procure assignment to the Buyer), title to and all rights and interest in the Specially Written Software together with and including:
        1. the Documentation, Source Code and the Object Code of the Specially Written Software; and
        2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software and the New IPR (together the **"Software Supporting Materials"**).
     2. The Supplier shall:
        1. inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;
        2. deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in an Implementation Plan, Achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and
        3. without prejudice to paragraph 9.1.2.2, provide full details to the Buyer of any of the Supplier’s Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Supplier’s Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.
     3. The Supplier shall promptly execute all such assignments as are required to ensure that any rights in the Specially Written Software and New IPRs are properly transferred to the Buyer.
  2. **Licences for non-COTS IPR from the Supplier and third parties to the Buyer**
     1. Unless the Buyer gives its Approval the Supplier must not use any:

1. of its own Existing IPR that is not COTS Software;
2. third party software that is not COTS Software
   * 1. Where the Buyer Approves the use of the Supplier’s Existing IPR that is not COTS Software the Supplier shall grant to the Buyer a perpetual, royalty-free and non-exclusive licence to use adapt, and sub-license the same for any purpose relating to the Deliverables (or substantially equivalent deliverables) or for any purpose relating to the exercise of the Buyer’s (or, if the Buyer is a Central Government Body, any other Central Government Body’s) business or function including the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display) for the Call Off Contract Period and after expiry of the Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.
     2. Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 9.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:
        1. notify the Buyer in writing giving details of what licence terms can be obtained and whether there are alternative software providers which the Supplier could seek to use; and
        2. only use such third party IPR as referred to at paragraph 9.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.
     3. Where the Supplier is unable to provide a license to the Supplier’s Existing IPR in accordance with Paragraph 9.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.
     4. The Supplier may terminate a licence granted under paragraph 9.2.1 by giving at least thirty (30) days’ notice in writing if there is an Authority Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.
   1. **Licenses for COTS Software by the Supplier and third parties to the Buyer**
      1. The Supplier shall either grant, or procure that the owners or the authorised licensors of any COTS Software grant, a direct licence to the Buyer on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.
      2. Where the Supplier owns the COTS Software it shall make available the COTS software to a Replacement Supplier at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.
      3. Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 9.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licencee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.
      4. The Supplier shall notify the Buyer within seven (7) days of becoming aware of any COTS Software which in the next thirty-six (36) months:
         1. will no longer be maintained or supported by the developer; or
         2. will no longer be made commercially available
   2. **Buyer’s right to assign/novate licences**
      1. The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to paragraph 9.2 (to:
         1. a Central Government Body; or
         2. to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer.
      2. If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in paragraph 9.2.
   3. **Licence granted by the Buyer**
      1. The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Buyer Software and the Specially Written Software solely to the extent necessary for providing the Deliverables in accordance with this Contract, including the right to grant sub-licences to Sub-Contractors provided that any relevant Sub-Contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 15 (Confidentiality).
   4. **Open Source Publication**
      1. Unless the Buyer otherwise agrees in advance in writing (and subject to paragraph 9.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:
         1. suitable for publication by the Buyer as Open Source; and
         2. based on Open Standards (where applicable),

and the Buyer may, at its sole discretion, publish the same as Open Source.

* + 1. The Supplier hereby warrants that the Specially Written Software and the New IPR:
       1. are suitable for release as Open Source and that the Supplier has used reasonable endeavours when developing the same to ensure that publication by the Buyer will not enable a third party to use them in any way which could reasonably be foreseen to compromise the operation, running or security of the Specially Written Software, New IPRs or the Buyer System;
       2. have been developed using reasonable endeavours to ensure that their publication by the Buyer shall not cause any harm or damage to any party using them;
       3. do not contain any material which would bring the Buyer into disrepute;
       4. can be published as Open Source without breaching the rights of any third party;
       5. will be supplied in a format suitable for publication as Open Source (**"the Open Source Publication Material"**) no later than the date notified by the Buyer to the Supplier; and
       6. do not contain any Malicious Software.
    2. Where the Buyer has Approved a request by the Supplier for any part of the Specially Written Software or New IPRs to be excluded from the requirement to be in an Open Source format due to the intention to embed or integrate Supplier Existing IPRs and/or Third Party IPRs (and where the Parties agree that such IPRs are not intended to be published as Open Source), the Supplier shall:
       1. as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Deliverables based on IPRs which are to be excluded from Open Source publication; and
       2. include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on such IPRs, will have on any other Specially Written Software and/or New IPRs and the Buyer’s ability to publish such other items or Deliverables as Open Source.
  1. **Malicious Software**
     1. The Supplier shall, throughout the Contract Period, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of Malicious Software.
     2. If Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any losses and to restore the provision of the Deliverables to its desired operating efficiency.
     3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of paragraph 9.7.2 shall be borne by the Parties as follows:
        1. by the Supplier, where the Malicious Software originates from the Supplier Software, the third party Software supplied by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and
        2. by the Buyer, if the Malicious Software originates from the Buyer Software or the Buyer Data (whilst the Buyer Data was under the control of the Buyer).

### IPR asset management

* 1. The Parties shall work together to ensure that there is appropriate IPR asset management under each Call-Off Contract, and:
     1. where the Supplier is working on the Buyer’s System, the Supplier shall comply with the Buyer’s IPR asset management approach and procedures.
     2. where the Supplier is working on the Supplier’s System, the Buyer will ensure that it maintains its IPR asset management procedures in accordance with Good Industry Practice.

Records and materials associated with IPR asset management shall form part of the Deliverables, including those relating to any Specially Written Software or New IPR.

* 1. The Supplier shall comply with any instructions given by the Buyer as to where it shall store all work in progress Deliverables and finished Deliverables (including all Documentation and Source Code) during the term of the Call-Off Contract and at the stated intervals or frequency specified by the Buyer and upon termination of the Contract or any Statement of Work.
  2. The Supplier shall ensure that all items it uploads into any repository contain sufficient detail, code annotations and instructions so that a third-party developer (with the relevant technical abilities within the applicable role) would be able to understand how the item was created and how it works together with other items in the repository within a reasonable timeframe.
  3. The Supplier shall maintain a register of all Open Source Software it has used in the provision of the Deliverables as part of its IPR asset management obligations under this Contract.

## Call-Off Schedule 7 (Key Supplier Staff)

### Key Supplier Staff

* 1. The Order Form lists the key roles (**“Key Roles”**) and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date and the Statement of Work lists the Key Roles and names of persons who the Supplier shall appoint to fill those Key Roles as of the SOW Start Date.
  2. The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.
  3. The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.
  4. The Supplier shall not remove or replace and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:
     1. requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);
     2. the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or
     3. the person’s employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.
  5. The Supplier shall:
     1. notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);
     2. ensure that any Key Role is not vacant for any longer than ten (10) Working Days;
     3. give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff’s employment contract, this will mean at least three (3) Months’ notice;
     4. ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables;
     5. ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced;
     6. on written request from the Buyer, provide a copy of the contract of employment or engagement (between the Supplier and Supplier Staff) for every member of the Supplier Staff made available to the Buyer under the Call-Off Contract when providing Deliverables under any Statement of Work; and
     7. on written request from the Buyer, provide details of start and end dates of engagement for all Key Staff filling Key Roles under any Statement of Work**.**
  6. The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff

## Call-Off Schedule 9 (Security)

### Part B: Long Form Security Requirements

### Definitions

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

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Breach of Security** | 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 Buyer 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 Buyer and/or the Supplier in connection with this Contract,   in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d; |
| **ISMS** | 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** | tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security. |

### Security Requirements

* 1. The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.
  2. The Parties acknowledge that the purpose of the ISMS and Security Management Plan 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. **Todd Samways, Todd.Samways100@mod.gov.uk**
     2. **Cheryl McMurray, CherylMcMurray@rowdentech.com**
  4. The Buyer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, 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 Buyer 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 Buyer requiring immediate communication and co-operation between the Parties.

### Information Security Management System (ISMS)

* 1. The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Start Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 3.4 to 3.6.
  2. The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.
  3. The Buyer acknowledges that;
     1. If the Buyer has not stipulated during a Further Competition that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier’s estate; and
     2. Where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer’s Approval.
  4. The ISMS shall:
     1. if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer 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 Buyer or the Supplier in connection with this Contract;
     2. meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;
     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;
3. as a minimum demonstrates Good Industry Practice;
4. where specified by a Buyer that has undertaken a Further Competition, complies with the Security Policy and the ICT Policy;
5. complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1 to 4) (<https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework>);
6. takes account of guidance issued by the Centre for Protection of National Infrastructure (<https://www.cpni.gov.uk>);
7. complies with HMG Information Assurance Maturity Model and Assurance Framework (<https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm>);
8. meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;
9. addresses issues of incompatibility with the Supplier’s own organisational security policies; and
10. complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;
    * 1. document the security incident management processes and incident response plans;
      2. document the vulnerability management policy including processes 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 security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and
      3. be certified by (or by a person with the direct delegated authority of) a Supplier’s main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).
    1. Subject to Paragraph 2 the references to Standards, guidance and policies contained or set out in Paragraph 3.4 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.
    2. In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.
    3. If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.3.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer 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 fifteen (15) Working Days from the date of the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable.
    4. Approval by the Buyer of the ISMS pursuant to Paragraph 3.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

### Security Management Plan

* 1. Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph 4 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.
  2. The Security Management Plan shall:
     1. be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);
     2. comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;
     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 Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer 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) and any system that could directly or indirectly have an impact on that information, data and/or the Deliverables;
     5. unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer 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 Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
     6. set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.4);
     7. demonstrate that the Supplier’s approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, ‘platform as a service’ offering from the G-Cloud catalogue);
     8. set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;
     9. set out the scope of the Buyer System that is under the control of the Supplier;
     10. be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and
     11. be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer 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.
  3. If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, 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 Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer 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 fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer 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 Buyer 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 4.2 shall be deemed to be reasonable.
  4. Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

### Amendment of the ISMS and Security Management Plan

* 1. The ISMS and 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. where required in accordance with paragraph 3.4.3 d, 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 Buyer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS 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 ISMS;
     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 ISMS; and
     4. suggested improvements in measuring the effectiveness of controls.
  3. Subject to Paragraph 5.4, 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 5.1, a Buyer 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 Buyer 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.

### Security Testing

* 1. The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. 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.
  2. The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.
  3. Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer 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 ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer’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.
  4. Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 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 Buyer of any changes to the ISMS 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 Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.
  5. If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

### Complying with the ISMS

* 1. The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3 d.
  2. If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer 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 Buyer 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 ISO/IEC 27001 and/or, where relevant, the Security Policy 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 Buyer in obtaining such audit.

### Security Breach

* 1. Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS 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 8.1, the Supplier shall:
     1. immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) 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 Buyer Property and/or Buyer Assets and/or ISMS 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 Service Level Performance Indicators, 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 Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) 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 Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.
   1. 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 ISMS with the Security Policy (where relevant) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Buyer.

### Vulnerabilities and fixing them

* 1. The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer’s information.
  2. The severity of threat vulnerabilities for COTS Software 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 ISMS 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 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.
  3. The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as ‘Critical’ within 14 days of release, ‘Important’ within 30 days of release and all ‘Other’ within 60 Working Days of release, except where:
     1. the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;
     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 Buyer; or
     3. the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.
  4. The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the ‘n-1 version’) throughout the Term unless:
     1. where upgrading such COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or
     2. is agreed with the Buyer in writing.
  5. The Supplier shall:
     1. implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;
     2. ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;
     3. ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;
     4. pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3.5;
     5. from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;
     6. propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;
     7. 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 the ICT Environment); and
     8. inform the Buyer 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.
  6. If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.
  7. A failure to comply with Paragraph 9.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

### Part B: Annex 1

### Baseline security requirements

### Handling Classified information

* 1. The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

### End user devices

* 1. When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the National Cyber Security Centre (“NCSC”) to at least Foundation Grade, for example, under the NCSC Commercial Product Assurance scheme ("CPA").
  2. Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a ‘known good’ state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (<https://www.ncsc.gov.uk/guidance/end-user-device-security>). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the NCSC guidance, then this should be agreed in writing on a case by case basis with the Buyer.

### Data Processing, Storage, Management and Destruction

* 1. The Supplier and Buyer recognise the need for the Buyer’s information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.
  2. The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).
  3. The Supplier shall:
     1. provide the Buyer with all Government Data on demand in an agreed open format;
     2. have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;
     3. securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and
     4. securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

### Ensuring secure communications

* 1. The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by NCSC, to at least Foundation Grade, for example, under CPA.
  2. The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

### Security by design

* 1. The Supplier shall apply the ‘principle of least privilege’ (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.
  2. When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a NCSC certification (<https://www.ncsc.gov.uk/section/products-services/ncsc-certification>) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

### Security of Supplier Staff

* 1. Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.
  2. The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as ‘SC’) including system administrators with privileged access to IT systems which store or process Government Data.
  3. The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.
  4. All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.
  5. Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

### Restricting and monitoring access

* 1. The Supplier shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the ‘principle of least privilege’, users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The Supplier shall retain an audit record of accesses.

### Audit

* 1. The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:
     1. Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.
     2. Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.
  2. The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.
  3. The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 Months.

### Part B: Annex 2

### Security Management Plan

## Call-Off Schedule 10 (Exit Management)

### Definitions

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

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Exclusive Assets** | Supplier Assets used exclusively by the Supplier **or a Key Subcontractor** in the provision of the Deliverables; |
| **Exit Information** | has the meaning given to it in Paragraph 3.1 of this Schedule; |
| **Exit Manager** | the person appointed by each Party to manage their respective obligations under this Schedule; |
| **Exit Plan** | the plan produced and updated by the Supplier during the Initial Period in accordance with Paragraph 4 of this Schedule; |
| **Net Book Value** | the current net book value of the relevant Supplier Asset(s) calculated in accordance with the Framework Tender or Call-Off Tender (if stated) or (if not stated) the depreciation policy of the Supplier (which the Supplier shall ensure is in accordance with Good Industry Practice); |
| **Non- Exclusive Assets** | those Supplier Assets used by the Supplier **or a Key Subcontractor** in connection with the Deliverables but which are also used by the Supplier **or Key Subcontractor** for other purposes; |
| **Registers** | the register and configuration database referred to in Paragraph 2.2 of this Schedule; |
| **Replacement Goods** | any goods which are substantially similar to any of the Goods and which the Buyer receives in substitution for any of the Goods following the End Date, whether those goods are provided by the Buyer internally and/or by any third party; |
| **Replacement Services** | any services which are substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services following the End Date, whether those goods are provided by the Buyer internally and/or by any third party; |
| **Termination Assistance** | the activities to be performed by the Supplier pursuant to the Exit Plan, and other assistance required by the Buyer pursuant to the Termination Assistance Notice; |
| **Termination Assistance Notice** | has the meaning given to it in Paragraph 5.1 of this Schedule; |
| **Termination Assistance Period** | the period specified in a Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to Paragraph 5.2 of this Schedule; |
| **Transferable Assets** | Exclusive Assets which are capable of legal transfer to the Buyer; |
| **Transferable Contracts** | Sub- Contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are necessary to enable the Buyer or any Replacement Supplier to provide the Deliverables or the Replacement Goods and/or Replacement Services, including in relation to licences all relevant Documentation; |
| **Transferring Assets** | has the meaning given to it in Paragraph 8.2.1 of this Schedule; and |
| **Transferring Contracts** | has the meaning given to it in Paragraph 8.2.3 of this Schedule. |

### Supplier must always be prepared for Contract exit and SOW exit

* 1. The Supplier shall within 30 days from the Call-Off Contract Start Date provide to the Buyer a copy of its depreciation policy to be used for the purposes of calculating Net Book Value.
  2. During the Contract Period, the Supplier shall promptly:
     1. create and maintain a detailed register of all Supplier Assets (including description, condition, location and details of ownership and status as either Exclusive Assets or Non-Exclusive Assets and Net Book Value) and Sub-contracts and other relevant agreements required in connection with the Deliverables; and
     2. create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Deliverables which will be stored in the Deliverables IPR asset management system which includes all Document and Source Code repositories.

("**Registers**").

* 1. The Supplier shall:
     1. ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and
     2. procure that all licences for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation (at no cost or restriction to the Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.
  2. Each Party shall appoint an Exit Manager within three (3) Months of the Call-Off Contract Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of each SOW and this Contract.

### Assisting re-competition for Deliverables

* 1. The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence whether this is in relation to one or more SOWs or the Call-Off Contract. (the "**Exit Information**").
  2. The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier’s or its Subcontractors’ prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.
  3. The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).
  4. The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Deliverables; and not be disadvantaged in any procurement process compared to the Supplier.

### Exit Plan

* 1. The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer a Call-Off Contract and SOW Exit Plan which complies with the requirements set out in Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.
  2. The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of the latest date for its submission pursuant to Paragraph 4.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
  3. The Exit Plan shall set out, as a minimum:
     1. a detailed description of both the transfer and cessation processes, including a timetable (this may require modification to SOW Exit Plan provisions to be updated and incorporated as part of the SOW;
     2. how the Deliverables will transfer to the Replacement Supplier and/or the Buyer;
     3. details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;
     4. proposals for the training of key members of the Replacement Supplier’s staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;
     5. proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;
     6. proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;
     7. proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;
     8. proposals for the disposal of any redundant Deliverables and materials;
     9. how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and
     10. any other information or assistance reasonably required by the Buyer or a Replacement Supplier.
  4. The Supplier shall:
     1. maintain and update the Exit Plan (and risk management plan) no less frequently than:

1. prior to each SOW and no less than every six (6) months throughout the Contract Period; and
2. no later than twenty (20) Working Days after a request from the Buyer for an up-to-date copy of the Exit Plan;
3. as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than ten (10) Working Days after the date of the Termination Assistance Notice;
4. as soon as reasonably possible following, and in any event no later than twenty (20) Working Days following, any material change to the Deliverables (including all changes under the Variation Procedure); and
   * 1. jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.
   1. Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.
   2. A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

### Termination Assistance

* 1. The Buyer shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a "**Termination Assistance Notice**") at least four (4) Months prior to the Expiry Date or, as soon as reasonably practicable, in the case of the Call-Off Contract and each SOW (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:
     1. the nature of the Termination Assistance required; and
     2. the start date and initial period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) Months after the End Date.
  2. The Buyer shall have an option to extend the Termination Assistance Period beyond the initial period specified in the Termination Assistance Notice in one or more extensions, in each case provided that:
     1. no such extension shall extend the Termination Assistance Period beyond the date twelve (12) Months after the End Date; and
     2. the Buyer shall notify the Supplier of any such extension no later than twenty (20) Working Days prior to the date on which the Termination Assistance Period is otherwise due to expire.
  3. The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier.
  4. In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

### Termination Assistance Period

* 1. Throughout the Termination Assistance Period the Supplier shall:
     1. continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;
     2. provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;
     3. use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;
     4. subject to Paragraph 6.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI’s) or Service Levels or KPIs, the provision of the Management Information or any other reports or to any other of the Supplier's obligations under this Contract;
     5. at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;
     6. seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.
  2. If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.
  3. If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Levels or KPIs, the Parties shall vary the relevant Service Levels and/or the KPIs accordingly.

### Obligations when the contract is terminated

* 1. The Supplier shall comply with all of its obligations contained in the Exit Plan.
  2. Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:
     1. vacate any Buyer Premises;
     2. remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;
     3. provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:

1. such information relating to the Deliverables as remains in the possession or control of the Supplier; and
2. such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier, provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.
   1. Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.

### Assets, Sub-contracts and Software

* 1. Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:
     1. terminate, enter into or vary any Sub-contract or licence for any software in connection with the Deliverables; or
     2. (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.
  2. Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out:
     1. which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("**Transferring Assets**");
     2. which, if any, of:

1. the Exclusive Assets that are not Transferable Assets; and
2. the Non-Exclusive Assets,

the Buyer and/or the Replacement Supplier requires the continued use of; and

* + 1. which, if any, of Transferable Contracts the Buyer requires to be assigned or novated to the Buyer and/or the Replacement Supplier (the "**Transferring Contracts**"),

in order for the Buyer and/or its Replacement Supplier to provide the Deliverables from the expiry of the Termination Assistance Period. The Supplier shall provide all reasonable assistance required by the Buyer and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts are required to provide the Deliverables or the Replacement Goods and/or Replacement Services.

* 1. With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Buyer and/or the Replacement Supplier for their Net Book Value less any amount already paid for them through the Charges.
  2. Risk in the Transferring Assets shall pass to the Buyer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.
  3. Where the Buyer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:
     1. procure a non-exclusive, perpetual, royalty-free licence for the Buyer and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which
     2. procure a suitable alternative to such assets, the Buyer or the Replacement Supplier to bear the reasonable proven costs of procuring the same.
  4. The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Buyer reasonably requires to effect this novation or assignment.
  5. The Buyer shall:
     1. accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and
     2. once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.
  6. The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.
  7. The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to Paragraph 8.6 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. Clause 19 (Other people's rights in this contract) shall not apply to this Paragraph 8.9 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

### No charges

* 1. Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

### Dividing the bills

* 1. All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:
     1. the amounts shall be annualised and divided by 365 to reach a daily rate;
     2. the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and
     3. the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

## Call-Off Schedule 13 (Implementation Plan and Testing)

### Part A: Implementation

### Definitions

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

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Delay** | 1. a delay in the Achievement of a Milestone by its Milestone Date; or 2. a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan; |
| **Deliverable Item** | an item or feature in the supply of the Deliverables delivered or to be delivered by the Supplier at or before a Milestone Date listed in the Implementation Plan; |
| **Milestone Payment** | a payment identified in the Implementation Plan to be made following the issue of a Satisfaction Certificate in respect of Achievement of the relevant Milestone; and |
| **Implementation Period** | has the meaning given to it in Paragraph 7.1. |

### Agreeing and following the implementation Plan

* 1. A draft of the Implementation Plan is set out in the Annex to this Schedule. The Supplier shall provide a further draft Implementation Plan 20 working days after the Call-Off Contract Start Date.
  2. The draft Implementation Plan:
     1. must contain information at the level of detail necessary to manage the implementation stage effectively for the whole Call-Off Contract and each Statement of Work issued under it for the supply of Deliverables and as the Buyer may otherwise require; and
     2. it shall take account of all dependencies known to, or which should reasonably be known to, the Supplier.
  3. Following receipt of the draft Implementation Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the Implementation Plan. If the Parties are unable to agree the contents of the Implementation Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
  4. The Supplier shall provide each of the Deliverable Items identified in the Implementation Plan by the date assigned to that Deliverable Item in the Implementation Plan so as to ensure that each Milestone identified in the Implementation Plan is achieved on or before its Milestone Date.
  5. The Supplier shall monitor its performance against the Implementation Plan and Milestones (if any) and report to the Buyer on such performance.
  6. The Supplier shall, in relation to each SOW, incorporate within it all Implementation Plan and Testing requirements for the satisfactory completion of each Deliverable Item to be provided under that SOW,

### Reviewing and changing the Implementation Plan

* 1. Subject to Paragraph 4.3, the Supplier shall keep the Implementation Plan under review in accordance with the Buyer’s instructions and ensure that it is updated on a regular basis.
  2. The Buyer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.
  3. Changes to any Milestones, Milestone Payments and Delay Payments shall only be made in accordance with the Variation Procedure.
  4. Time in relation to compliance with the Implementation Plan shall be of the essence and failure of the Supplier to comply with the Implementation Plan shall be a material Default.

### Security requirements before the Start Date

* 1. The Supplier shall note that it is incumbent upon them to understand the lead-in period for security clearances and ensure that all Supplier Staff have the necessary security clearance in place before the Call-Off Start Date. The Supplier shall ensure that this is reflected in their Implementation Plans.
  2. The Supplier shall ensure that all Supplier Staff and Subcontractors do not access the Buyer's IT systems, or any IT systems linked to the Buyer, unless they have satisfied the Buyer's security requirements.
  3. The Supplier shall be responsible for providing all necessary information to the Buyer to facilitate security clearances for Supplier Staff and Subcontractors in accordance with the Buyer's requirements.
  4. The Supplier shall provide the names of all Supplier Staff and Subcontractors and inform the Buyer of any alterations and additions as they take place throughout the Call-Off Contract.
  5. The Supplier shall ensure that all Supplier Staff and Subcontractors requiring access to the Buyer Premises have the appropriate security clearance. It is the Supplier's responsibility to establish whether or not the level of clearance will be sufficient for access. Unless prior approval has been received from the Buyer, the Supplier shall be responsible for meeting the costs associated with the provision of security cleared escort services.
  6. If a property requires Supplier Staff or Subcontractors to be accompanied by the Buyer’s Authorised Representative, the Buyer must be given reasonable notice of such a requirement, except in the case of emergency access.

### What to do if there is a Delay

* 1. If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay under this Contract it shall:
     1. notify the Buyer as soon as practically possible and no later than within two (2) Working Days from becoming aware of the Delay or anticipated Delay;
     2. include in its notification an explanation of the actual or anticipated impact of the Delay;
     3. comply with the Buyer’s instructions in order to address the impact of the Delay or anticipated Delay; and
     4. use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay.

### Compensation for a Delay

* 1. If Delay Payments have been included in the Implementation Plan and a Milestone has not been achieved by the relevant Milestone Date, the Supplier shall pay to the Buyer such Delay Payments (calculated as set out by the Buyer in the Implementation Plan) and the following provisions shall apply:
     1. the Supplier acknowledges and agrees that any Delay Payment is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier’s failure to Achieve the corresponding Milestone;
     2. Delay Payments shall be the Buyer's exclusive financial remedy for the Supplier’s failure to Achieve a Milestone by its Milestone Date except where:

1. the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (When CCS or the Buyer can end this contract); or
2. the delay exceeds the number of days (the "**Delay Period Limit**") specified in the Implementation Plan commencing on the relevant Milestone Date;
   * 1. the Delay Payments will accrue on a daily basis from the relevant Milestone Date until the date when the Milestone is Achieved;
     2. no payment or other act or omission of the Buyer shall in any way affect the rights of the Buyer to recover the Delay Payments or be deemed to be a waiver of the right of the Buyer to recover any such damages; and
     3. Delay Payments shall not be subject to or count towards any limitation on liability set out in Clause 11 (How much you can be held responsible for).

### Implementation Plan

* 1. The Implementation Period will be a six (6) Month period for the Call-Off Contract and for the duration of each SOW.
  2. During the Implementation Period, the incumbent supplier shall retain full responsibility for all existing services until the Call-Off Start Date or as otherwise formally agreed with the Buyer in each SOW. The Supplier's full service obligations shall formally be assumed on the Call-Off Start Date as set out in Order Form.
  3. In accordance with the Implementation Plan, the Supplier shall:
     1. work cooperatively and in partnership with the Buyer, incumbent supplier, and other Framework Supplier(s), where applicable, to understand the scope of Services to ensure a mutually beneficial handover of the Services;
     2. work with the incumbent supplier and Buyer to assess the scope of the Services and prepare a plan which demonstrates how they will mobilise the Services;
     3. liaise with the incumbent Supplier to enable the full completion of the Implementation Period activities; and
     4. produce a Implementation Plan, to be agreed by the Buyer, for carrying out the requirements within the Implementation Period including, key Milestones and dependencies.
  4. The Implementation Plan will include detail stating:
     1. how the Supplier will work with the incumbent Supplier and the Buyer Authorised Representative to capture and load up information such as asset data; and
     2. a communications plan, to be produced and implemented by the Supplier, but to be agreed with the Buyer, including the frequency, responsibility for and nature of communication with the Buyer and end users of the Services.
  5. In addition, the Supplier shall:
     1. appoint a Supplier Authorised Representative who shall be responsible for the management of the Implementation Period, to ensure that the Implementation Period is planned and resourced adequately, and who will act as a point of contact for the Buyer;
     2. mobilise all the Services specified in the Specification within the Call-Off Contract and each SOW;
     3. produce a Implementation Plan report for each Buyer Premises to encompass programmes that will fulfil all the Buyer's obligations to landlords and other tenants:

1. the format of reports and programmes shall be in accordance with the Buyer's requirements and particular attention shall be paid to establishing the operating requirements of the occupiers when preparing these programmes which are subject to the Buyer's approval; and
2. the Parties shall use reasonable endeavours to agree the contents of the report but if the Parties are unable to agree the contents within twenty (20) Working Days of its submission by the Supplier to the Buyer, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
   * 1. manage and report progress against the Implementation Plan both at a Call-Off Contract level (which shall include an update on costings) and SOW level;
     2. construct and maintain a Implementation risk and issue register in conjunction with the Buyer detailing how risks and issues will be effectively communicated to the Buyer in order to mitigate them;
     3. attend progress meetings (frequency of such meetings shall be as set out in the Order Form and each SOW) in accordance with the Buyer's requirements during the Implementation Period. Implementation meetings shall be chaired by the Buyer and all meeting minutes shall be kept and published by the Supplier; and
     4. ensure that all risks associated with the Implementation Period are minimised to ensure a seamless change of control between incumbent provider and the Supplier.

#### Annex 1: Implementation Plan

A.1 The Supplier shall provide a:

1. high level Implementation Plan for the Call-Off Contract as part of the Further Competition Procedure; and
2. a detailed Implementation Plan for each SOW.

A.2 The Implementation Plan is set out below and the Milestones to be Achieved are identified below:

* Milestone: [ ]
* Deliverable Items: [ ]
* Duration: [ ]
* Milestone Date: [ ]
* Buyer Responsibilities: [ ]
* Milestone Payments: [ ]
* Delay Payments: [ ]

The Milestones will be Achieved in accordance with this Call-Off Schedule 13: (Implementation Plan and Testing)

For the purposes of Paragraph 6.1.2 the Delay Period Limit shall be 90 days.

### Part B: Testing

### Definitions

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

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Component** | any constituent parts of the Deliverables; |
| **Material Test Issue** | a Test Issue of Severity Level 1 or Severity Level 2; |
| **Satisfaction Certificate** | a certificate materially in the form of the document contained in Annex 2 issued by the Buyer when a Deliverable and/or Milestone has satisfied its relevant Test Success Criteria; |
| **Severity Level** | the level of severity of a Test Issue, the criteria for which are described in Annex 1; |
| **Test Issue Management Log** | a log for the recording of Test Issues as described further in Paragraph 8.1 of this Schedule; |
| **Test Issue Threshold** | in relation to the Tests applicable to a Milestone, a maximum number of Severity Level 3, Severity Level 4 and Severity Level 5 Test Issues as set out in the relevant Test Plan; |
| **Test Reports** | the reports to be produced by the Supplier setting out the results of Tests; |
| **Test Specification** | the specification that sets out how Tests will demonstrate that the Test Success Criteria have been satisfied, as described in more detail in Paragraph 6.2 of this Schedule; |
| **Test Strategy** | a strategy for the conduct of Testing as described further in Paragraph 3.2 of this Schedule; |
| **Test Success Criteria** | in relation to a Test, the test success criteria for that Test as referred to in Paragraph 5 of this Schedule; |
| **Test Witness** | any person appointed by the Buyer pursuant to Paragraph 9 of this Schedule; and |
| **Testing Procedures** | the applicable testing procedures and Test Success Criteria set out in this Schedule. |

### How testing should work

* 1. All Tests conducted by the Supplier shall be conducted in accordance with the Test Strategy, Test Specification and the Test Plan.
  2. The Supplier shall not submit any Deliverable for Testing:
     1. unless the Supplier is reasonably confident that it will satisfy the relevant Test Success Criteria;
     2. until the Buyer has issued a Satisfaction Certificate in respect of any prior, dependant Deliverable(s); and
     3. until the Parties have agreed the Test Plan and the Test Specification relating to the relevant Deliverable(s).
  3. The Supplier shall use reasonable endeavours to submit each Deliverable for Testing or re-Testing by or before the date set out in the Implementation Plan for the commencement of Testing in respect of the relevant Deliverable.
  4. Prior to the issue of a Satisfaction Certificate, the Buyer shall be entitled to review the relevant Test Reports and the Test Issue Management Log.

### Planning for testing

* 1. The Supplier shall develop the final Test Strategy as soon as practicable after the Start Date but in any case no later than twenty (20) Working Days after the Start Date.
  2. The final Test Strategy shall include:
     1. an overview of how Testing will be conducted in relation to the Implementation Plan;
     2. the process to be used to capture and record Test results and the categorisation of Test Issues;
     3. the procedure to be followed should a Deliverable fail a Test, fail to satisfy the Test Success Criteria or where the Testing of a Deliverable produces unexpected results, including a procedure for the resolution of Test Issues;
     4. the procedure to be followed to sign off each Test;
     5. the process for the production and maintenance of Test Reports and a sample plan for the resolution of Test Issues;
     6. the names and contact details of the Buyer and the Supplier's Test representatives;
     7. a high level identification of the resources required for Testing including Buyer and/or third party involvement in the conduct of the Tests;
     8. the technical environments required to support the Tests; and
     9. the procedure for managing the configuration of the Test environments.

### Preparing for Testing

* 1. The Supplier shall develop Test Plans and submit these for Approval as soon as practicable but in any case no later than twenty (20) Working Days prior to the start date for the relevant Testing as specified in the Implementation Plan.
  2. Each Test Plan shall include as a minimum:
     1. the relevant Test definition and the purpose of the Test, the Milestone to which it relates, the requirements being Tested and, for each Test, the specific Test Success Criteria to be satisfied; and
     2. a detailed procedure for the Tests to be carried out.
  3. The Buyer shall not unreasonably withhold or delay its approval of the Test Plan provided that the Supplier shall implement any reasonable requirements of the Buyer in the Test Plan.

### Passing Testing

* 1. The Test Success Criteria for all Tests shall be agreed between the Parties as part of the relevant Test Plan pursuant to Paragraph 4.

### How Deliverables will be tested

* 1. Following approval of a Test Plan, the Supplier shall develop the Test Specification for the relevant Deliverables as soon as reasonably practicable and in any event at least 10 Working Days prior to the start of the relevant Testing (as specified in the Implementation Plan).
  2. Each Test Specification shall include as a minimum:
     1. the specification of the Test data, including its source, scope, volume and management, a request (if applicable) for relevant Test data to be provided by the Buyer and the extent to which it is equivalent to live operational data;
     2. a plan to make the resources available for Testing;
     3. Test scripts;
     4. Test pre-requisites and the mechanism for measuring them; and
     5. expected Test results, including:

1. a mechanism to be used to capture and record Test results; and
2. a method to process the Test results to establish their content.

### Performing the tests

* 1. Before submitting any Deliverables for Testing the Supplier shall subject the relevant Deliverables to its own internal quality control measures.
  2. The Supplier shall manage the progress of Testing in accordance with the relevant Test Plan and shall carry out the Tests in accordance with the relevant Test Specification. Tests may be witnessed by the Test Witnesses in accordance with Paragraph 9.3.
  3. The Supplier shall notify the Buyer at least 10 Working Days in advance of the date, time and location of the relevant Tests and the Buyer shall ensure that the Test Witnesses attend the Tests.
  4. The Buyer may raise and close Test Issues during the Test witnessing process.
  5. The Supplier shall provide to the Buyer in relation to each Test:
     1. a draft Test Report not less than 2 Working Days prior to the date on which the Test is planned to end; and
     2. the final Test Report within 5 Working Days of completion of Testing.
  6. Each Test Report shall provide a full report on the Testing conducted in respect of the relevant Deliverables, including:
     1. an overview of the Testing conducted;
     2. identification of the relevant Test Success Criteria that have/have not been satisfied together with the Supplier's explanation of why any criteria have not been met;
     3. the Tests that were not completed together with the Supplier's explanation of why those Tests were not completed;
     4. the Test Success Criteria that were satisfied, not satisfied or which were not tested, and any other relevant categories, in each case grouped by Severity Level in accordance with Paragraph 8.1; and
     5. the specification for any hardware and software used throughout Testing and any changes that were applied to that hardware and/or software during Testing.
  7. When the Supplier has completed a Milestone it shall submit any Deliverables relating to that Milestone for Testing.
  8. Each party shall bear its own costs in respect of the Testing. However, if a Milestone is not Achieved the Buyer shall be entitled to recover from the Supplier, any reasonable additional costs it may incur as a direct result of further review or re-Testing of a Milestone.
  9. If the Supplier successfully completes the requisite Tests, the Buyer shall issue a Satisfaction Certificate as soon as reasonably practical following such successful completion. Notwithstanding the issuing of any Satisfaction Certificate, the Supplier shall remain solely responsible for ensuring that the Deliverables are implemented in accordance with this Contract.

### Discovering Problems

* 1. Where a Test Report identifies a Test Issue, the Parties shall agree the classification of the Test Issue using the criteria specified in Annex 1 and the Test Issue Management Log maintained by the Supplier shall log Test Issues reflecting the Severity Level allocated to each Test Issue.
  2. The Supplier shall be responsible for maintaining the Test Issue Management Log and for ensuring that its contents accurately represent the current status of each Test Issue at all relevant times. The Supplier shall make the Test Issue Management Log available to the Buyer upon request.
  3. The Buyer shall confirm the classification of any Test Issue unresolved at the end of a Test in consultation with the Supplier. If the Parties are unable to agree the classification of any unresolved Test Issue, the Dispute shall be dealt with in accordance with the Dispute Resolution Procedure using the Expedited Dispute Timetable.

### Test witnessing

* 1. The Buyer may, in its sole discretion, require the attendance at any Test of one or more Test Witnesses selected by the Buyer, each of whom shall have appropriate skills to fulfil the role of a Test Witness.
  2. The Supplier shall give the Test Witnesses access to any documentation and Testing environments reasonably necessary and requested by the Test Witnesses to perform their role as a Test Witness in respect of the relevant Tests.
  3. The Test Witnesses:
     1. shall actively review the Test documentation;
     2. will attend and engage in the performance of the Tests on behalf of the Buyer so as to enable the Buyer to gain an informed view of whether a Test Issue may be closed or whether the relevant element of the Test should be re-Tested;
     3. shall not be involved in the execution of any Test;
     4. shall be required to verify that the Supplier conducted the Tests in accordance with the Test Success Criteria and the relevant Test Plan and Test Specification;
     5. may produce and deliver their own, independent reports on Testing, which may be used by the Buyer to assess whether the Tests have been Achieved;
     6. may raise Test Issues on the Test Issue Management Log in respect of any Testing; and
  4. may require the Supplier to demonstrate the modifications made to any defective Deliverable before a Test Issue is closed.

### Auditing the quality of the test

* 1. The Buyer or an agent or contractor appointed by the Buyer may perform on-going quality audits in respect of any part of the Testing (each a "**Testing Quality Audit**") subject to the provisions set out in the agreed Quality Plan.
  2. The Supplier shall allow sufficient time in the Test Plan to ensure that adequate responses to a Testing Quality Audit can be provided.
  3. The Buyer will give the Supplier at least 5 Working Days' written notice of the Buyer’s intention to undertake a Testing Quality Audit.
  4. The Supplier shall provide all reasonable necessary assistance and access to all relevant documentation required by the Buyer to enable it to carry out the Testing Quality Audit.
  5. If the Testing Quality Audit gives the Buyer concern in respect of the Testing Procedures or any Test, the Buyer shall prepare a written report for the Supplier detailing its concerns and the Supplier shall, within a reasonable timeframe, respond in writing to the Buyer’s report.
  6. In the event of an inadequate response to the written report from the Supplier, the Buyer (acting reasonably) may withhold a Satisfaction Certificate until the issues in the report have been addressed to the reasonable satisfaction of the Buyer.

### Outcome of the testing

* 1. The Buyer will issue a Satisfaction Certificate when the Deliverables satisfy the Test Success Criteria in respect of that Test without any Test Issues.
  2. If the Deliverables (or any relevant part) do not satisfy the Test Success Criteria then the Buyer shall notify the Supplier and:
     1. the Buyer may issue a Satisfaction Certificate conditional upon the remediation of the Test Issues;
     2. the Buyer may extend the Test Plan by such reasonable period or periods as the Parties may reasonably agree and require the Supplier to rectify the cause of the Test Issue and re-submit the Deliverables (or the relevant part) to Testing; or
     3. where the failure to satisfy the Test Success Criteria results, or is likely to result, in the failure (in whole or in part) by the Supplier to meet a Milestone, then without prejudice to the Buyer’s other rights and remedies, such failure shall constitute a material Default.
  3. The Buyer shall be entitled, without prejudice to any other rights and remedies that it has under this Contract, to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing which is required for the Test Success Criteria for that Deliverable to be satisfied.
  4. The Buyer shall issue a Satisfaction Certificate in respect of a given Milestone as soon as is reasonably practicable following:
     1. the issuing by the Buyer of Satisfaction Certificates and/or conditional Satisfaction Certificates in respect of all Deliverables related to that Milestone which are due to be Tested; and
     2. performance by the Supplier to the reasonable satisfaction of the Buyer of any other tasks identified in the Implementation Plan as associated with that Milestone.
  5. The grant of a Satisfaction Certificate shall entitle the Supplier to the receipt of a payment in respect of that Milestone in accordance with the provisions of any Implementation Plan and Clause 4 (Pricing and payments).
  6. If a Milestone is not Achieved, the Buyer shall promptly issue a report to the Supplier setting out the applicable Test Issues and any other reasons for the relevant Milestone not being Achieved.
  7. If there are Test Issues but these do not exceed the Test Issues Threshold, then provided there are no Material Test Issues, the Buyer shall issue a Satisfaction Certificate.
  8. If there is one or more Material Test Issue(s), the Buyer shall refuse to issue a Satisfaction Certificate and, without prejudice to the Buyer’s other rights and remedies, such failure shall constitute a material Default.
  9. If there are Test Issues which exceed the Test Issues Threshold but there are no Material Test Issues, the Buyer may at its discretion (without waiving any rights in relation to the other options) choose to issue a Satisfaction Certificate conditional on the remediation of the Test Issues in accordance with an agreed Rectification Plan provided that:
     1. any Rectification Plan shall be agreed before the issue of a conditional Satisfaction Certificate unless the Buyer agrees otherwise (in which case the Supplier shall submit a Rectification Plan for approval by the Buyer within 10 Working Days of receipt of the Buyer’s report pursuant to Paragraph 10.5); and
     2. where the Buyer issues a conditional Satisfaction Certificate, it may (but shall not be obliged to) revise the failed Milestone Date and any subsequent Milestone Date.

### Risk

* 1. The issue of a Satisfaction Certificate and/or a conditional Satisfaction Certificate shall not:
     1. operate to transfer any risk that the relevant Deliverable or Milestone is complete or will meet and/or satisfy the Buyer’s requirements for that Deliverable or Milestone; or
     2. affect the Buyer’s right subsequently to reject all or any element of the Deliverables and/or any Milestone to which a Satisfaction Certificate relates.

### Annex 1: Test Issues, Severity Levels

### Severity 1 Error

* 1. This is an error that causes non-recoverable conditions, e.g. it is not possible to continue using a Component.

### Severity 2 Error

* 1. This is an error for which, as reasonably determined by the Buyer, there is no practicable workaround available, and which:
     1. causes a Component to become unusable;
     2. causes a lack of functionality, or unexpected functionality, that has an impact on the current Test; or
     3. has an adverse impact on any other Component(s) or any other area of the Deliverables;

### Severity 3 Error

* 1. This is an error which:
     1. causes a Component to become unusable;
     2. causes a lack of functionality, or unexpected functionality, but which does not impact on the current Test; or
     3. has an impact on any other Component(s) or any other area of the Deliverables;

but for which, as reasonably determined by the Buyer, there is a practicable workaround available;

### Severity 4 Error

* 1. This is an error which causes incorrect functionality of a Component or process, but for which there is a simple, Component based, workaround, and which has no impact on the current Test, or other areas of the Deliverables.

### Severity 5 Error

* 1. This is an error that causes a minor problem, for which no workaround is required, and which has no impact on the current Test, or other areas of the Deliverables.

### Annex 2: Satisfaction Certificate

To: **[insert name of Supplier]**

From: **[insert name of Buyer]**

**[insert Date dd/mm/yyyy]**

Dear Sirs,

**Satisfaction Certificate**

Deliverable/Milestone(s): **[Insert relevant description of the agreed Deliverables/Milestones].**

We refer to the agreement ("**Call-Off Contract"**) **[insert Call-Off Contract reference number and any applicable SOW reference]** relating to the provision of the **[insert description of the Deliverables]** between the **[insert Buyer name]** ("**Buyer**") and **[insert Supplier name**] ("**Supplier**") dated **[insert Call-Off Start Date dd/mm/yyyy]**.

The definitions for any capitalised terms in this certificate are as set out in the Call-Off Contract.

[We confirm that all the Deliverables relating to **[insert relevant description of Deliverables/agreed Milestones and/or reference number(s) from the Implementation Plan]** have been tested successfully in accordance with the Test Plan [or that a conditional Satisfaction Certificate has been issued in respect of those Deliverables that have not satisfied the relevant Test Success Criteria].

**[OR]**

[This Satisfaction Certificate is granted on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]

[You may now issue an invoice in respect of the Milestone Payment associated with this Milestone in accordance with Clause 4 (Pricing and payments)].

Yours faithfully

**[insert Name]**

**[insert Position]**

acting on behalf of **[insert name of Buyer**

## Call-Off Schedule 17 (MOD Terms)

### Definitions

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

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **MOD Terms and Conditions** | the terms and conditions listed in this Schedule; |
| **MOD Site** | shall include any of Her Majesty's Ships or Vessels and Service Stations; and |
| **Officer in charge** | shall include Officers Commanding Service Stations, Ships' Masters or Senior Officers, and Officers superintending Government Establishments. |

### Access to MOD sites

* 1. The Buyer shall issue passes for those representatives of the Supplier who are approved for admission to the MOD Site and a representative shall not be admitted unless in possession of such a pass. Passes shall remain the property of the Buyer and shall be surrendered on demand or on completion of the supply of the Deliverables.
  2. The Supplier's representatives when employed within the boundaries of a MOD Site, shall comply with such rules, regulations and requirements (including those relating to security arrangements) as may be in force for the time being for the conduct of staff at that MOD Site. When on board ship, compliance shall be with the Ship's Regulations as interpreted by the Officer in charge. Details of such rules, regulations and requirements shall be provided, on request, by the Officer in charge.
  3. The Supplier shall be responsible for the living accommodation and maintenance of its representatives while they are employed at a MOD Site. Sleeping accommodation and messing facilities, if required, may be provided by the Buyer wherever possible, at the discretion of the Officer in charge, at a cost fixed in accordance with current Ministry of Defence regulations. At MOD Sites overseas, accommodation and messing facilities, if required, shall be provided wherever possible. The status to be accorded to the Supplier's staff for messing purposes shall be at the discretion of the Officer in charge who shall, wherever possible give his decision before the commencement of this Contract where so asked by the Supplier. When sleeping accommodation and messing facilities are not available, a certificate to this effect may be required by the Buyer and shall be obtained by the Supplier from the Officer in charge. Such certificate shall be presented to the Buyer with other evidence relating to the costs of this Contract.
  4. Where the Supplier's representatives are required by this Contract to join or visit a Site overseas, transport between the United Kingdom and the place of duty (but excluding transport within the United Kingdom) shall be provided for them free of charge by the Ministry of Defence whenever possible, normally by Royal Air Force or by MOD chartered aircraft. The Supplier shall make such arrangements through the Technical Branch named for this purpose in the Buyer Contract Details. When such transport is not available within a reasonable time, or in circumstances where the Supplier wishes its representatives to accompany material for installation which it is to arrange to be delivered, the Supplier shall make its own transport arrangements. The Buyer shall reimburse the Supplier's reasonable costs for such transport of its representatives on presentation of evidence supporting the use of alternative transport and of the costs involved. Transport of the Supplier's representatives locally overseas which is necessary for the purpose of this Contract shall be provided wherever possible by the Ministry of Defence, or by the Officer in charge and, where so provided, shall be free of charge.
  5. Out-patient medical treatment given to the Supplier's representatives by a Service Medical Officer or other Government Medical Officer at a Site overseas shall be free of charge. Treatment in a Service hospital or medical centre, dental treatment, the provision of dentures or spectacles, conveyance to and from a hospital, medical centre or surgery not within the Site and transportation of the Supplier's representatives back to the United Kingdom, or elsewhere, for medical reasons, shall be charged to the Supplier at rates fixed in accordance with current Ministry of Defence regulations.
  6. Accidents to the Supplier's representatives which ordinarily require to be reported in accordance with Health and Safety at Work etc. Act 1974, shall be reported to the Officer in charge so that the Inspector of Factories may be informed.
  7. No assistance from public funds, and no messing facilities, accommodation or transport overseas shall be provided for dependants or members of the families of the Supplier's representatives. Medical or necessary dental treatment may, however, be provided for dependants or members of families on repayment at current Ministry of Defence rates.
  8. The Supplier shall, wherever possible, arrange for funds to be provided to its representatives overseas through normal banking channels (e.g. by travellers' cheques). If banking or other suitable facilities are not available, the Buyer shall, upon request by the Supplier and subject to any limitation required by the Supplier, make arrangements for payments, converted at the prevailing rate of exchange (where applicable), to be made at the Site to which the Supplier's representatives are attached. All such advances made by the Buyer shall be recovered from the Supplier

### DEFCONS and DEFFORMS

* 1. The DEFCONS and DEFORMS listed in Annex 1 to this Schedule are incorporated into this Contract.
  2. Where a DEFCON or DEFORM is updated or replaced the reference shall be taken as referring to the updated or replacement DEFCON or DEFORM from time to time.
  3. In the event of a conflict between any DEFCONs and DEFFORMS listed in the Order Form and the other terms in a Call Off Contract, the DEFCONs, DEFFORMS and terms in Call-Off Schedule 17 shall prevail.

### Authorisation by the Crown for use of third party intellectual property rights

* 1. Notwithstanding any other provisions of the Call Off Contract and for the avoidance of doubt, award of the Call Off Contract by the Buyer and placement of any contract task under it does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977 or Section 12 of the Registered Designs Act 1949. The Supplier acknowledges that any such authorisation by the Buyer under its statutory powers must be expressly provided in writing, with reference to the acts authorised and the specific intellectual property involved.

### Intellectual property rights and Additional Terms on Digital Deliverables

* 1. Further to clause 9 of Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables), the Supplier shall take all necessary measures to irrevocably and unconditionally waive in favour of the Buyer any and all moral rights and all other non-assignable rights conferred on the Supplier’s employees and sub-contractors in-respect of any copyright work created in carrying out the Contract. On request, the Supplier shall demonstrate to the Buyer’s satisfaction that, where it has sub-contracted work under the Contract, it has secured that any and all moral rights in any copyright work created by the Supplier’s employees and its sub-contractors has been irrevocably and unconditionally waived in favour of the Buyer.
  2. Further to clause 9.2.2 of Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables), the licence granted to the Buyer by the Supplier shall include the right to modify the Supplier’s Existing IPR that is not COTS Software. And, the Supplier shall deliver to the Buyer any and all Supplier’s Existing IPR which forms all or part of a Deliverable.
  3. Further clause 9.2.3 of Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables), the direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 9.2.2. shall include the right to modify the third party’s IPR that is not COTS Software. And, the supplier will deliver to the Buyer any and all third party IPR which forms all or part of a Deliverable.
  4. Clause 9.3.1 of Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables) is disapplied and in its stead the following shall apply:

9.3.1 Unless the Buyer gives its Approval the Supplier must not use any of its own existing COTS Software or third-party COTS Software. Where the Buyer Approves the use of the Supplier’s COTS Software or third-party COTS Software, the Supplier shall either grant, or procure that the owners or the authorised licensors of any COTS Software grant, a direct licence to the Buyer in the form of a DEFFORM 701.  If the Supplier cannot obtain such a licence for the Buyer, it shall notify the Buyer in writing giving details of what licence terms can be obtained and whether there are alternative software providers which the Supplier could seek to use.

* 1. Clause 9.3.2 of Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables) is disapplied.
  2. Clause 9.6.1 of Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables) is disapplied and in its stead the following shall apply:

9.6.1 All Specially Written Software and computer program elements of New IPR shall be created in a format, or converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:

9.6.1.1 suitable for publication by the Buyer as Open Source; and

9.6.1.2 based on Open Standards (where applicable), and the Buyer may, at its sole discretion, publish the same as Open Source.

* 1. Clause 9.6.3 of Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables) is disapplied.

### ANNEX 1: DEFCONS and DEFFORMS

The full text of Defence Conditions (DEFCONs) and Defence Forms (DEFFORMS) are at: <https://www.gov.uk/acquisition-operating-framework>.

The following MOD DEFCONs and DEFFORMs form part of this contract:

#### DEFCONs

|  |  |  |
| --- | --- | --- |
| **DEFCON No** | **Version** | **Description** |
| DEFCON 23 | Edn 06/21 | Special Jigs, Tooling and Test Equipment |
| DEFCON 76 | Edn 06/21 | Contractor’s Personnel at Government Establishments |
| DEFCON 129J | Edn 18/11/16 | The Use of the Electronic Business Delivery Form |
| DEFCON 611 | Edn 02/16 | Issued Property |
| DEFCON 656A | Edn 08/16 | Termination for Convenience – Under £5M |
| DEFCON 660 | Edn 12/15 | Official-Sensitive Security Requirements |
| DEFCON 694 | Edn 07/21 | Accounting for Property of the Authority |

#### DEFFORMs (Ministry of Defence Forms)

|  |  |  |
| --- | --- | --- |
| **DEFFORM No** | **Version** | **Description** |
| DEFFORM 94 | Edn 12/20 | Confidentiality Agreement |
| DEFFORM 701 | Edn 06/21 | Head Agreement For Licence Terms for Commercial Software Purchased By The Secretary Of State For Defence |

## Call-Off Schedule 18 (Background Checks)

### When you should use this Schedule

This Schedule should be used where Supplier Staff must be vetted before working on the Contract.

### Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Relevant Conviction** | means any conviction listed in Annex 1 to this Schedule. |

### Relevant Convictions

* 1. The Supplier must ensure that no person who discloses that they have a Relevant Conviction, or a person who is found to have any Relevant Convictions (whether as a result of a police check or through the procedure of the Disclosure and Barring Service (DBS) or otherwise), is employed or engaged in any part of the provision of the Deliverables without Approval.
  2. Notwithstanding Paragraph 3.1 for each member of Supplier Staff who, in providing the Deliverables, has, will have or is likely to have access to children, vulnerable persons or other members of the public to whom the Buyer owes a special duty of care, the Supplier must (and shall procure that the relevant Sub-Contractor must):

1. carry out a check with the records held by the Department for Education (DfE);
2. conduct thorough questioning regarding any Relevant Convictions; and
3. ensure a police check is completed and such other checks as may be carried out through the Disclosure and Barring Service (DBS),

and the Supplier shall not (and shall ensure that any Sub-Contractor shall not) engage or continue to employ in the provision of the Deliverables any person who has a Relevant Conviction or an inappropriate record.

### Annex 1: Relevant Convictions

The following are classed as a Relevant Conviction for the purpose of this Call-Off Contract:

(a) conspiracy within the meaning of section 1 or section 1A of the Criminal Law Act 1977 or article 9 or 9A of the Criminal Attempts and Conspiracy (Northern Ireland) Order 1983, or in Scotland the Offence of conspiracy, where that conspiracy relates to participation in a criminal organisation as defined in Article 2 of Council Framework Decision 2008/841/JHA;

(b) involvement in serious organised crime or directing serious organised crime within the meaning of section 28 or 30 of the Criminal Justice and Licensing (Scotland) Act 2010;

(c) corruption within the meaning of section 1 of the Public Bodies Corrupt Practices Act 1889 or section 1 of the Prevention of Corruption Act 1906\*;

(d) the offence of bribery;

(e) bribery within the meaning of section 1, 2 or 6 of the Bribery Act 2010;

(f) bribery or corruption within the meaning of section 68 and 69 of the Criminal Justice (Scotland) Act 2003;

(g) money laundering within the meaning of section 93A, 93B, or 93C of the Criminal Justice Act 1988, section 45, 46 or 47 of the Proceeds of Crime (Northern Ireland) Order 1996 or the Money Laundering Regulations 2003 or money laundering or terrorist financing within the meaning of the Money Laundering Regulations 2007\*;

(h) terrorist offences or offences linked to terrorist activities, as defined in Articles 1 and 3 of Framework Decision 2002/475/JHA\*;

(i) an offence in connection with proceeds of drug trafficking within the meaning of section 49, 50 or 51 of the Drug Trafficking Act 1994.

\*including amendments to the legislation.

## Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract.

|  |  |
| --- | --- |
|  |  |

DEFENCE DIGITAL: SERVICE DELIVERY & OPERATIONS

**DISMOUNTED SITUATIONAL AWARENESS (DSA)**

**Design and Integration Partner**

**Statement of Requirement Document**

**Version 1.0**

|  |  |
| --- | --- |
| Project Name: | DISMOUNTED SITUATIONAL AWARENESS |
| Date: | 01/03/2021 |
| Author: | Toni Reed |
| Owner: | Ed Roberts (ISS Dev-BATCIS-DSA AsstHd-PPM) |
| Document Number: |  |

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision No.** | **Revision Date** | **Brief Revision Description** | **Change Control** |
| 1.0 | 01/03/2021 | Version 1.0 for release to industry |  |

Approvals

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Name** | **Role** | **Date** |
| Prepared by: | Toni Reed | DSA Procurement Lead | 01/03/2021 |
| Reviewed by: | Adrian Smith | DSA System Engineer Lead | 01/03/2021 |
| Approved & Authorised by: | Edward Roberts | DSA Senior PM | 01/03/2021 |

Peer Review

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** | **Date** |
|  |  |  |
|  |  |  |
|  |  |  |

References

1. DSA User Requirements Document (available upon request to shortlisted suppliers)
2. DSA Background Technical Information Document (available upon request to shortlisted suppliers)
3. Draft DSA System Architecture (available at Contract Award)
4. Draft Joint Relationship Management Plan (available at Contract Award)
5. AQAP 2110 - NATO Quality Assurance Requirements for Design, Development and Production, Edition D, Version 1 (publicly available)
6. AQAP 2210 - NATO Supplementary Software Quality Assurance Requirements to AQAP 2110, Edition A, Version 2 (publicly available)
7. DEFSTAN 05-061 - Concessions. All concessions shall be managed in accordance with DEFSTAN 05-061, Part 1, Issue 6 (publicly available)
8. DEFSTAN 05-061 - Contractor's working parties. Any contract working parties shall be provided in accordance with DEFSTAN 05-061, Part 4 Issue 3 (publicly available)
9. DEFSTAN 05-099 Managing Government Furnished Equipment in Industry (publicly available)
10. DEFSTAN 05-057 Configuration Management of Defence Material (publicly available)
11. DOS 5 Call-Off Schedule 10 - Exit Management (publicly available)
12. Knowledge in Defence Portal[[1]](#footnote-2) (publicly accessible)
13. Draft System Requirements Document (available at Contract Award)
14. DEFSTAN 23-009 - General Vehicle Architecture (publicly available)
15. DEFSTAN 23-012 - Generic Solider Architecture (publicly available)
16. DEFSTAN 23-013 - Generic Base Architecture (publicly available)
17. BATCIS Electromagnetic Environmental Effects Requirements and Management Policy (available at Contract Award)
18. [Mission Service Assurance Approach to Land Environment Tactical Communications and Information Systems (LE TacCIS)](https://eur01.safelinks.protection.outlook.com/ap/w-59584e83/?url=https%3A%2F%2Fmodgovuk.sharepoint.com%2F%3Aw%3A%2Fr%2Fteams%2F13028%2FManProg%2FMSASG%2F20201102-LE%2520TacCIS_MSA_Approach-v1.0-SRO-O.docx%3Fd%3Dw62df264815894ebca8196f7b5defb64d%26csf%3D1%26web%3D1%26e%3D4XcYlZ&data=04%7C01%7CToni.Reed772%40mod.gov.uk%7C654d1b746eb2470f6cc408d88adc4d4c%7Cbe7760ed5953484bae95d0a16dfa09e5%7C0%7C0%7C637412026075106054%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=F7N2CNGiNyjd7fV8bEwo0ItutNaJMeXDR7L86AFvN%2FY%3D&reserved=0) (available at Contract Award)
19. Knowledge in Defence Guidance[[2]](#footnote-3): Software requirements including direction on contracting for software support, SRD and URDs (publicly available)
20. Knowledge in Defence Guidance: Generic software support requirements[[3]](#footnote-4) (publicly available)
21. Knowledge in Defence Guidance: Software Support Plans[[4]](#footnote-5) (publicly available)
22. ITIL Framework Service Management Strategy, V4 (publicly available)
23. Defence Digital Operations HQ OSM Context Document (available at Contract Award)
24. DSA Concept of Employment (available at Contract Award)
25. IEC 62402:2019 - Obsolescence Management (publicly available)
26. The Authority’s System Engineering Management Plan (available at Contract Award)
27. DOS 5 Framework Core Terms (publicly available)
28. Joint Schedule 2 of the DOS 5 Framework - Variation Form (publicly available)
29. DSA Integrated Test, Evaluation and Acceptance Plan (available at Contract Award)
30. DSA System Part 1) Safety and Environmental Case Report (available at Contract Award)
31. Safety Standard DEFSTAN 00-056 - Safety Management Requirements for Defence Systems (publicly available)
32. DEFSTAN 00-051 - Environmental Management Requirements for Defence Systems Requirements (publicly available)
33. Safety Standard DEFSTAN 00-055 - Requirements for Safety of Programmable Elements (PE) in Defence Systems (for System Functional Safety implemented via Software, Hardware and Firmware) (publicly available)
34. Safety and Environmental Regulation DSA02 (available at Contract Award)
35. Safety and Environmental Regulation DSA03 (available at Contract Award)
36. DSA System Safety and Environmental Management Plan (available at Contract Award)
37. The Authority's Security Management Plan (available at Contract Award)
38. Product Description for Supplier SMP (available at Contract Award)
39. Accreditation, Security Assurance and Risk Management artefacts (available at Contract Award)
40. DSA Accreditation Strategy (available at Contract Award)
41. Accreditation Evidence Statement (available at Contract Award)
42. Security Aspects Letters - Radio Provider (not yet developed)
43. Snapshot Technical Risk Assessment (available at Contract Award)
44. In-House Threat Assessment (available at Contract Award)
45. Security Risk Register (available at Contract Award)
46. Risk Treatment Plan (available at Contract Award)
47. CDO - External Governance Requirements (to be advised by the Authority as required).
48. MOD Internal Policy and Governance (available at Contract Award)
49. HMG - Good Practice Guides (to be advised by the Authority as required - publicly available)
50. HMG - Security Policy Framework (publicly available)
51. HMG - IAS I&2 (publicly available)
52. BS EN ISO 27001/2-2017 - Information technology. Security Techniques. Information Security Management Systems. Requirements (publicly available)
53. CDO Security Assurance Framework (available at Contract Award)
54. The Authority’s Integrated Logistics Support Plan (available at Contract Award)
55. DSA Technical Publications (not yet developed)

Glossary

|  |  |
| --- | --- |
| **Acronym** | **Explanation** |
| APM | Association for Project Management |
| Agile | Agile project management is an iterative approach to delivering a project throughout its life cycle |
| AQAP | Allied Quality Assurance Publications |
| AV | Anti-Virus |
| AWARD | A Commerce Decisions tool used by the Authority in competitive procurements; helps buyers to confidently and efficiently select the best supplier |
| BAFO | Best And Final Offer |
| BATCIS | Battlefield and Tactical Communications and Information Systems |
| BCIP | Bowman, Common Battlefield Applications Toolset (ComBAT), Infrastructure and Platform Battlefield Information Systems Applications |
| BS EN | British Standards European Norm |
| CA | Certification Authority |
| CADMID | Concept, Assessment, Demonstration, Manufacture, In Service, Disposal |
| CDD | Capability Delivery Drop |
| CDO | Coordinating Design Organisation |
| COEIA | Combined Operational Effectiveness and Investment Appraisal |
| ComBAT | Bowman, Common Battlefield Applications Toolset |
| DC3I | Dismounted Command, Control, Communications and Information |
| DEFSTAN | Defence Standard |
| DOORS | Dynamic Object-Oriented Requirements System |
| DOS | Digital Outcomes and Specialists |
| DPQQ | Dynamic Pre-Qualification Questionnaire |
| DR | Disaster Recovery |
| DSA | Dismounted Situational Awareness |
| E3 | Electromagnetic Environmental Effects |
| ECD | Evolutionary Capability Delivery |
| A Continual Service Improvement approach aimed at delivering optimal Return on Investment. Progressive evolution of the system, where each change results in a deliberate capability enhancement and/or other benefits realisation and is a transitional step on a trajectory towards a goal state. |
| ECM | Electronic Countermeasures |
| EMC | Electromagnetic Compatibility |
| FBC | Full Business Case |
| FP | Force Protection |
| GFA | Government Furnished Assets |
| HFI | Human Factors Integration |
| HMG | Her Majesty's Government |
| IAS | Information Assurance Standard |
| IDAM | Identity & Access Management |
| IDR | Interim Design Review |
| IEC | International Electrotechnical Commission |
| ISO | International Organization for Standardization; |
| IT | Information Technology |
| ITEAP | Integrated Test, Evaluation and Acceptance Plan |
| ITHC | Information Technology Health Checks |
| ITIL | IT Infrastructure Library |
| JRMP | Joint Relationship Management Plan |
| KiD | Knowledge in Defence |
| KMTA | Key Management Trust Anchors |
| LE TacCIS | Land Environment Tactical Communications and Information Systems |
| MI | Mutual Interference |
| MOD | Ministry Of Defence |
| NATO | North Atlantic Treaty Organisation |
| OTS | Off-The-Shelf |
| PCT | Performance, Cost and Time |
| PDR | Preliminary Design Review |
| PKI | Public Key Infrastructure |
| PRINCE2 | Projects in Controlled Environments 2 - A structured project management method and practitioner certification programme. |
| PRR | Personal Role Radios |
| PSE | Platform, System, or Equipment |
| RA | Registration Authority |
| RadHaz | Radiation Hazard |
| RAIDO | Risk, Assumption, Issue, Dependency, Opportunity |
| RAMP | Requirements and Management Policy |
| RSDR | Radio Subsystem Design Review |
| RF | Radio Frequency |
| RMADS | Risk Management and Accreditation Document Sets |
| ROADs | Record of Actions and Decisions |
| ROM | Rough Order of Magnitude |
| SC | Security Check |
| SDA | System Design Authority |
| SDR | System Design Review |
| S&EMP | Safety and Environmental Management Plan |
| SEMS | Safety and Environmental Management System |
| SLA | Service Level Agreement |
| SMP | Security Management Plan |
| SSRD | Sub-System Requirement Document |
| SRD | System Requirements Document |
| SRR | System Requirements Review |
| SUKEO | Secret UK Eyes Only |
| SWG | Security Working Group |
| TEMPEST | The phenomena of unintentionally compromising sensitive information through electromagnetic emanations |
| UK | United Kingdom |
| URD | User Requirements Document |
| USA | United States of America |
| Vendor Lock in | Being constrained or tied to vendor/set of vendors' products or services due to proprietary issues or substantial switching costs associated with changing vendors |
| X509 | X.509 is a standard format for public key certificates |

Contents

[Revision History 72](#_Toc65748282)

[Approvals 72](#_Toc65748283)

[Peer Review 72](#_Toc65748284)

[References 73](#_Toc65748285)

[Glossary 75](#_Toc65748286)

[Contents 77](#_Toc65748287)

[DISMOUNTED SITUATIONAL AWARENESS (DSA) DESIGN & INTEGRATION PARTNER STATEMENT OF REQUIREMENT DOCUMENT 78](#_Toc65748288)

[DOCUMENT PURPOSE & RELATIONSHIP TO OTHER DOCUMENTS 78](#_Toc65748289)

[PROJECT OVERVIEW 78](#_Toc65748290)

[BACKGROUND 79](#_Toc65748291)

[OUTCOMES 79](#_Toc65748292)

[OVERARCHING REQUIREMENT 80](#_Toc65748293)

[SCOPE OF DESIGN & INTEGRATION PARTNER CONTRACT 80](#_Toc65748294)

[CONTEXT 81](#_Toc65748295)

[001 - PROJECT & PROGRAMME MANAGEMENT 82](#_Toc65748296)

[002 - REQUIREMENTS, ARCHITECTURE, DESIGN & ENGINEERING 85](#_Toc65748297)

[003 - SUPPORT TO AUTHORITY COMPETITIONS 91](#_Toc65748298)

[004 - MANAGE CHANGE CONTROL & CONFIGURATION MANAGEMENT 92](#_Toc65748299)

[005 - MANAGE SYSTEM INTEGRATION 93](#_Toc65748300)

[006 - SYSTEM DESIGN AUTHORITY (SDA), SYSTEM SAFETY & SYSTEM SECURITY 94](#_Toc65748301)

[007 - ADDITIONAL AD-HOC TASKING 100](#_Toc65748302)

[008 - SUPPORT TO TRAINING, INTRODUCTION TO SERVICE & LOGISTICS SUPPORT 100](#_Toc65748303)

[CONTRACT OPTIONS 101](#_Toc65748304)

[Annex A - Consolidated view of the Meetings, Deliverables and Supporting Activities associated with the Authority's Statement of Requirement 102](#_Toc65748305)

[Annex B - Record of Government Furnished Assets issued to the Design and Integration Partner 107](#_Toc65748306)

DISMOUNTED SITUATIONAL AWARENESS (DSA) DESIGN & INTEGRATION PARTNER STATEMENT OF REQUIREMENT DOCUMENT

DOCUMENT PURPOSE & RELATIONSHIP TO OTHER DOCUMENTS

1. This document sets out the business requirements for the future capability to be delivered by the DSA Design and Integration Partner. It provides an overview of the DSA project, describes the roles and responsibilities of the Design and Integration Partner and outlines the expected relationships between the Authority, the Design and Integration Partner and other third-party suppliers delivering the DSA capability.
2. A consolidated view of the meetings, deliverables, supporting activities and the Authority's indicative timeframes associated with this Statement of Requirement document can be found at Annex A. The Design and Integration Partner and the Authority shall work collaboratively to produce realistic and achievable timelines for delivery. Annex A shall be updated with the deliverable timeframes agreed between both parties at Contract Award.
3. This document does not detail the User Requirements of the DSA system; this can be found in the DSA User Requirements Document (URD) [reference A]. The URD should be read in conjunction with this document and shall be issued to shortlisted suppliers upon request.
4. The DSA Background Technical Information Document [reference B] provides further information of the work conducted to date and should also be read in conjunction with this document. The DSA Background Technical Information Document shall be issued to shortlisted suppliers upon request.
5. A full list of referenced documents, standards and frameworks can be found in the reference section above. Some referenced documents, standards and frameworks may not be available for release at Contract Award and may be developed alongside the delivery of work within this Statement of Requirement (these have been clearly identified and are for information only at this time).
6. The following sections of this document are for information only and have been included to provide the Design and Integration Partner with the context of the entire DSA project:
7. Project Overview.
8. Background.
9. Outcomes.
10. Overarching Requirement.

PROJECT OVERVIEW

1. Availability of situational awareness information in a timely, accurate and consistent manner is a key enabler to the effective command and control of dismounted close combat forces and achievement of military objectives. The United Kingdom’s (UK's) current use of paper maps and radio voice communications is slow and onerous and can lead to misinterpretations between commanders. Advances in situational awareness technology, as demonstrated by the United States of America (USA) and other allies, offer the opportunity to further digitise the Battlefield. Through the automation of battlefield data collation and exploitation, commanders at company-level[[5]](#footnote-6) and below, shall be more informed, able to make decisions quicker, increasing operational tempo and reducing the risk of own force casualties.
2. The DSA project team entered an Assessment Phase[[6]](#footnote-7) in March 2021 to develop a new, technology-driven, situational awareness capability enabled through the acquisition of suitably qualified and experienced industry partners. Specifically, a Design and Integration Partner to develop a Ministry Of Defence (MOD) owned solution which shall enable future capability evolution into the 2030s and beyond, ensuring that the MOD has access to the latest technology and innovation from across industry whilst avoiding "Vendor Lock In[[7]](#footnote-8)". A Radio Provider and component provider[[8]](#footnote-9) shall also be contracted by the Authority to provide/manufacture/produce the physical DSA system at scale. It is expected the first capability delivery of DSA shall be Quarter 2 2024.
3. DSA is a project within the Land Environment Tactical Communications and Information Systems (LE TacCIS) Programme. The DSA project team sits within the Dismounted Command, Control, Communications and Information (DC3I) team. As part of Battlefield and Tactical Communications and Information Systems (BATCIS) delivery team it reports to Defence Digital, Directorate Information and Ground Manoeuvre.

BACKGROUND

1. The complexities of terrain, populations and enemy strategies within the Land Domain means that dismounted[[9]](#footnote-10) close combat remains a typical operational deployment. The achievement of military objectives through dismounted close combat operations, typically in a dispersed group, is dependent upon effective command and control enabled through situational awareness. Situational awareness is the: *“knowledge and understanding of the current situation which promotes timely, relevant and accurate assessment of friendly, competitive and other operations within the Battlefield in order to facilitate decision making. An informational perspective and skill that fosters an ability to determine quickly the context and relevance of events that are unfolding”*.
2. Today, the UK achieves situational awareness through the use of paper maps and radio communications, typically Personal Role Radios (PRR), with basic position location information provided by Bowman Common Battlefield Applications Toolset (ComBAT), Infrastructure and Platform Battlefield Information Systems Applications (BCIP) 5.6.
3. The need for more dependable battlefield situational awareness has been recognised for some time.
4. Through capability concept demonstrators in 2015 and 2019, the potential of technology to provide more timely, accurate, complete and consistent information, increasing dismounted commanders’ decision-making capabilities and an overall significant step-change in military effectiveness has been demonstrated.
5. For UK Defence to realise the operational benefits of this technology, the DSA project was established to provide dismounted close combat users with enhanced voice and data services that shall result in greater situational awareness capabilities.

OUTCOMES

1. The primary outcomes of the DSA project are to visualise battlefield information, reduce the burden of collating operational data and provide military commanders timely data to make better, more accurate operational decisions. Benefits include:
2. Increased tempo, by enabling a wealth of position location information to be gathered and presented automatically and more accurately in seconds, compared to the current more manual process often undertaken over congested voice communications networks.
3. Better and quicker decisions, by reducing the information gathering process and decreasing the cognitive burden on commanders allowing them to focus on analysing the available information to make quicker, better informed decisions.
4. Increased coordination, by providing a battlefield management view of operations and a means of planning and communicating across forces without having to rely on voice communications, reducing errors and confusion.
5. Reduction in risk and own force casualties, by enabling users to locate and communicate more accurately both enemy and friendly force locations, reducing the risk of fratricide.
6. Optimised communications performance by managing the electromagnetic integration of DSA to maintain safety, security and co-site interoperability.

OVERARCHING DSA REQUIREMENT

1. The DSA project shall provide an Official Sensitive[[10]](#footnote-11) capability incorporating:
2. Voice communications, i.e. radios, to all dismounted close combat users.
3. Situational awareness to all dismounted commanders to company-level, including:
4. Position and location information of soldiers.
5. Friendly force locations.
6. Battlefield management software applications, including visual representations, operational constraints and intelligence.
7. Planning and information sharing tools for commanders.
8. Ability to work collaboratively between commanders within the company group.
9. Ability to produce a coherent view of the battlefield and contribute to the strategic operational picture in a timely and accurate manner.
10. In simplified terms, DSA shall address: Where am I? Where is my unit? Where is the enemy? What are my orders?
11. Dismounted close combat users operate within a wide range of Radio Frequency (RF) environments, and as such, it is essential that the DSA capability continues to operate within the harshest of RF environments; which may include other co-sited transmitters and/or Force Protection (FP) Electronic Countermeasures (ECM).
12. The DSA capability shall be designed around the dismounted close combat soldier and allow future integration with mounted close combat[[11]](#footnote-12) platforms. In order to ensure effectiveness and compatibility with other technology-driven soldier related capabilities, its development shall be aligned to other MOD systems architecture and open standards.

SCOPE OF DESIGN & INTEGRATION PARTNER CONTRACT

1. The Authority requires a Design and Integration Partner to develop a MOD owned DSA solution, which shall enable future capability evolution into the 2030s and beyond, ensuring that the MOD has access to the latest technology and innovation from across industry whilst avoiding "Vendor Lock In". The Authority shall work collaboratively with the Design and Integration Partner to achieve this.
2. **Commercial construct:** The supplier who is awarded the Design and Integration Partner contract (and any parent company, subsidiary, sister company, affiliate or division of this organisation) shall NOT be eligible to bid for the DSA equipment supply contracts or make up any part of the supply chain of these contracts.
3. **Contract length:** The Design and Integration Partner contract shall be a 24-month core contract, to support the Authority with the Assessment Phase activity required up to DSA Full Business Case (FBC) approval, with a 6 month option for continuation of services, including exit and transition activities (as detailed at para 114 below), which may be exercised (or not) at the Authority's discretion.
4. The key business requirements for the DSA Design and Integration Partner are:
5. **001 - Programme and Project Management:** Manage the delivery of the contract in line with the processes and procedures in this document.
6. **002 - Requirements, Architecture, Design and Engineering:** Evolve and manage the draft DSA System Architecture [reference C] provided by the Authority (at Contract Award). Develop and manage the detailed DSA System Design, adapting the baselines in response to capability roadmaps, technology innovation, emerging user needs, system threats and/or system obsolescence. Assessment of Electromagnetic Integration. Produce DSA subsystem requirements documents, interface control documents, technical product specifications and supporting technical drawings/diagrams/documents in accordance with the DSA System Design. Support the Authority with the development of a Technical Library to host technical documentation and standards. Develop an Engineering Management Plan to set the engineering direction.
7. **003 - Support to Authority Competitions:** Support the Authority in the development of appropriate competition documentation and provide support to the Authority's competition process.
8. **004 - Manage Change Control:** Maintain and control the configuration of the DSA System Architecture, DSA System Design, and technical baselines on behalf of the Authority, ensuring on-going system openness.
9. **005 - Manage System Integration:** Manage all system integration activities, including planning, management and system acceptance testing for the duration of the contract.
10. **006 - System Design Authority, System Safety & System Security:** Responsible for System Design Authority (SDA) governance, including development and management of SDA processes/procedures. Produce and contribute to System Safety Cases and provide support to the Authority with Security Accreditation and Assurance activities.
11. **007 - Additional ad-hoc tasking:** Carry out additional ad-hoc taskings as agreed between the Authority and the Design and Integration Partner.
12. **008 - Support to Training, Introduction to Service & Logistics Support:** Provide support to the Authority with its training, introduction to service and logistics support activities.

CONTEXT

1. The Design and Integration Partner shall be responsible for the design and development of the DSA System, including evolving the draft DSA System Architecture and developing and managing the DSA System Design. The Design and Integration Partner shall produce detailed subsystem requirements documents and technical product specifications for the radio and components, which shall be used by the Authority to contract third party suppliers to provide/manufacture/produce the DSA system at scale:
2. The radio subsystem requirements documents and technical product specifications shall form the basis of the procurement for a Radio Provider, the competition for which shall be led by the Authority supported by the Design and Integration Partner. The competition shall include down-select trials to ensure that the chosen radio, together with associated waveforms and cryptographic security, can perform at the required operational level and environment. The Design and Integration Partner shall support the Authority with these down-select trials.
3. The component subsystem requirements documents and technical product specifications shall be used by the Authority to contract for the supply of components.
4. The Design and Integration Partner shall work with the Authority (and its third-party suppliers) to scope solution designs which ensure optimised value for money for the DSA system.
5. Once the radio and component solutions have been selected, they shall be presented to an Authority led design board[[12]](#footnote-13), along with the corresponding Combined Operational Effectiveness and Investment Appraisals (COEIAs), for approval at FBC.
6. The Design and Integration Partner shall provide the required support to the Authority up to and including the FBC submission. The Design and Integration Partner shall conduct exit activities and transition the Design and Integration Partner services to the Authority and/or an incoming supplier prior to contract expiry.

Diagram

Description automatically generated

Figure 1 - Collaborative Working Relationship across DSA

1. Effective collaborative working between the Design and Integration Partner, the Authority, the Authority's third-party suppliers, as well as Authority stakeholders shall be crucial to the success of the DSA project (see Figure 1 above).

**LE TACCIS PROGRAMME APPROACH**

1. **Evolutionary Capability Delivery (ECD)**: The LE TacCIS Programme is taking a continual service improvement approach towards delivering capability. ECD will achieve deliberate capability enhancement and/or other LE TacCIS Programme benefits, through progressive evolution of systems. The Design and Integration Partner shall design the DSA System to enable this incremental approach to achieve the benefits offered by ECD. The DSA URD covers the full scope of delivery for the DSA project.
2. **Capability Delivery Drops**: The Authority’s approach to delivering the DSA solution and achieving ECD benefits will be through Capability Delivery Drops (CDDs). The Authority shall agree the scope of each CDD as part of an options analysis process. Further detail on this approach can be found in the DSA Background Technical Information Document.

001 - PROJECT & PROGRAMME MANAGEMENT

1. **Delivery of the contract:** The Design and Integration Partner shall project manage the delivery of the contract in line with the processes and procedures set out in this section.
2. **Onboarding:** At Contract Award, the Design and Integration Partner shall provide the Authority with its personnel information (numbers, roles and experience, Security Clearance[[13]](#footnote-14) details) and sign any Non-Disclosure Agreements issued by the Authority to allow the Authority to make the necessary access arrangements (site access, Information Technology (IT) access etc). The Authority shall provide the Design and Integration Partner personnel with the necessary technical and project information, including induction training (where required). The Design and Integration Partner shall attend a project kick-off meeting (hosted and chaired by the Authority) to agree communication methods between the Authority and the Design and Integration Partner, clarify project timelines, discuss relationship management, confirm deliverables and objectives and ensure alignment from both parties from the start. The project kick-off meeting shall take place within 2 weeks of Contract Award.
3. **Collaborative working relationship:** The Design and Integration Partner and the Authority shall adopt a collaborative working relationship, which shall be described, implemented and managed through a Joint Relationship Management Plan (JRMP). This is a joint artefact, developed by both parties and is both a joint management platform incorporating a record of the approaches and agreements undertaken to the point of formalising the collaboration, and a relationship platform for ongoing management of the relationship. The JRMP is a dynamic document for use throughout the lifetime of the contract. A draft version of the JRMP [reference D] shall be issued to the Design and Integration Partner at Contract Award. An updated version of the JRMP is to be agreed and signed by both parties within 1 month of Contract Award.
4. **Collaborative working behaviours:** The Design and Integration Partner shall:
5. Raise any problems, issues or risks to the delivery of the project to the Authority at the earliest opportunity; which shall be handled and managed jointly between the Authority and Design and Integration Partner.
6. Cooperate with the Authority and the Authority's third-party suppliers, stakeholders and representatives, in the delivery of the contract.
7. Work with the parties at para 33b to establish key governance, management and reporting mechanisms, and support activities required by the project (including cross-project/programme activities, where so required by the Authority).
8. Support and attend all required activities and meetings at either the Authority's premises or host activities and meetings at the Design and Integration Partner's premises (where so required by the Authority).
9. **Multilateral Joint Relationship Management (when/if required):** The Design and Integration Partner shall support the Authority with the introduction of the Authority's third-party suppliers, to a multilateral joint relationship. The Design and Integration Partner shall attend meetings in support of this multilateral joint relationship and contribute to the Authority's development of Multilateral JRMPs.
10. **Reporting & Governance (to commence post project kick-off meeting):** The Design and Integration Partner shall support the Authority with its reporting and governance activities. This shall include attendance and contribution at project meetings, as follows:
11. Project and technical desk level contribution and attendance required at weekly, monthly and quarterly project meetings/boards.
12. Expected topics for discussion shall include (but shall not be limited to):
13. Risk, assumption, issue, dependency and opportunity management.
14. Progress against the schedule and project milestones.
15. Performance management.
16. Project configuration management.
17. Quality management.
18. Business relationship management.
19. Information knowledge management.
20. Learning from experience and continuous improvement.
21. The Authority shall send out the calling-notice for all project meetings. The venue of the project meetings shall be jointly agreed between the Authority and Design and Integration Partner. Actions, minutes and decisions shall be taken and distributed by the Authority (if required), with progress reviewed at the next corresponding project meeting. Any preparatory work/input required from the Design and Integration Partner shall be communicated by the Authority in advance of each project meeting.
22. **Risk, Assumption, Issue, Dependency, Opportunity (RAIDO) management:** The Design and Integration Partner shall manage RAIDO activity in line with Association for Project Management (APM)/PRINCE[[14]](#footnote-15)2 best practice. The Design and Integration Partner shall support the Authority in developing and maintaining the DSA RAIDO register, which shall be hosted on the Authority's shared working environment, contribute to active risk management of the project, and provide status updates at the project meetings detailed above.
23. **Project Planning & Scheduling**: The Design and Integration Partner shall develop and manage planning and scheduling activity in line with best practice (e.g. APM/Agile/PRINCE2) and input/provide support to the development of the DSA Collaborative Master Schedule, which shall be hosted on the Authority's shared working environment. Both parties shall have access to all planning information, including how planning activity is being managed (processes and procedures), and shall provide progress updates into the DSA Collaborative Master Schedule.
24. **Quality Management:** The Design and Integration Partner shall comply with the following Quality Assurance requirements:
25. Allied Quality Assurance Publication (AQAP) 2110 - North Atlantic Treaty Organisation (NATO) Quality Assurance Requirements for Design, Development and Production, Edition D, Version 1 [reference E].
26. AQAP 2210 - NATO Supplementary Software Quality Assurance Requirements to AQAP 2110, Edition A, Version 2 [reference F].
27. Defence Standard (DEFSTAN) 05-061 - Concessions. All concessions shall be managed in accordance with DEFSTAN 05-061, Part 1, Issue 6 [reference G].
28. DEFSTAN 05-061 - Contractor's working parties. Any contract working parties shall be provided in accordance with DEFSTAN 05-061, Part 4 Issue 3 [reference H].
29. The Design and Integration Partner shall provide support to any quality audit conducted by the Authority and/or Defence Digital Quality Assurance representatives and identify and implement any corrective actions raised at the earliest opportunity. Progress shall be reviewed at the next corresponding project meeting.
30. **Information Knowledge Management:** The Design and Integration Partner shall share knowledge and best practise and support the Authority with identification and implementation of process improvements throughout the delivery of the contract. The Design and Integration Partner shall comply with the Authority's restrictions and handling instructions relating to storage of information in the Authority's shared working environment. The Design and Integration Partner shall ensure that personnel delivering the contract are appropriately trained and have the necessary expertise to perform their role.
31. **Import and Export Management:** The Design and Integration Partner shall inform the Authority of any and all import and export control agreements (and associated matters) which arise during the delivery of the contract and maintain a log of all such agreements.
32. **Management of Government Furnished Assets:** The Design and Integration Partner shall manage Government Furnished Assets (GFA) issued by the Authority in line with DEFSTAN 05-099 Managing Government Furnished Equipment in Industry [reference I] and DEFSTAN 05-057 Configuration Management of Defence Material [reference J]. The Authority shall provide the Design and Integration Partner with access to the BATCIS floorplate (as Government Furnished Facilities), including access to SECRET UK EYES ONLY (SUKEO) information. Annex B to this document lists the GFA to be issued (by the Authority) to the Design and Integration Partner[[15]](#footnote-16).
33. **Assurance, Approvals and Assessment Phase activity:** The Design and Integration Partner shall provide support to the Authority in its assurance, approvals and Assessment Phase activities, including but not limited to:
34. Support to the Authority in the development of Reports.
35. Support to the Authority in the development of Business Cases and Review Notes.
36. Support to the Authority in the development of Assurance and Approvals documentation.
37. Support to the Authority in the development of COEIAs.
38. **Supplier Service Transition and Offboarding:** The Design and Integration Partner shall conduct all service transition and offboarding activity as detailed in their Exit Plan (as per the requirements of the Digital Outcomes and Specialists (DOS) 5 Call-Off Schedule 10 (Exit Management) [reference K]).
39. The above processes and ways of working shall be subject to amendment as the collaborative relationship between the Authority and the Design and Integration Partner develops, and improvements to the processes, procedures and way of working are identified, agreed and adapted by both parties during delivery of the contract.

002 - REQUIREMENTS, ARCHITECTURE, DESIGN & ENGINEERING

1. The Authority requires a DSA system that works together (interoperates) with other complex systems, is vendor agnostic and achieves flexibility and commonality (where required); a modular system, where changes can be made to individual components/sub-systems within the overall design/system.
2. The Design and Integration Partner shall follow the guidance set out in the Knowledge in Defence (KiD) Portal [reference L]. The KiD Portal sets out the end-to-end processes associated with this Statement of Requirement, including but not limited to technical requirements and information on:
   1. Solution System Architecture.
   2. Requirements definition.
   3. Design documentation.
   4. Detailed specifications.
   5. Verified integration.
   6. Acceptance activities.
3. The Design and Integration Partner shall ensure all technical documentation produced maintains the ‘golden thread’ from User Requirements to System Design to Acceptance.
4. **Requirements Management**[[16]](#footnote-17): The Design and Integration Partner shall support the Authority through the Requirements and Acceptance end-to-end process. The Design and Integration Partner shall review the requirements documentation provided by the Authority (at Contract Award) and support the Authority in concluding the requirements definition activities.
5. **System Requirements Document (SRD):** The draft SRD [reference M] shall be provided by the Authority at Contract Award. The Design and Integration Partner shall support the Authority with development of this document, and it shall be baselined by the Authority at the System Requirements Review (detailed at para 61 below).
6. **DSA System Architecture**: At Contract Award the Authority shall issue the Design and Integration Partner with the draft DSA System Architecture[[17]](#footnote-18) . The Design and Integration Partner shall, with support from the Authority, evolve the draft DSA System Architecture, and provide an updated DSA System Architecture[[18]](#footnote-19) at Preliminary Design Review (detailed at para 61 below).
7. The DSA System Architecture documentation shall include but shall not be limited to:
8. Technical Drivers.
9. Constraints, dependencies, assumptions.
10. The DSA System Architecture shall be aligned to wider MOD systems architecture and open standards, including but not limited to:
11. DEFSTAN 23-009 - General Vehicle Architecture [reference N].
12. DEFSTAN 23-012 - Generic Solider Architecture [reference O].
13. DEFSTAN 23-013 - Generic Base Architecture [reference P].
14. The DSA System Architecture shall be agreed and baselined at the Formal Design Reviews (detailed at para 61 below). The Design and Integration Partner shall continue to develop and manage the DSA System Architecture throughout the duration of the contract.
15. **DSA System Design:** The Design and Integration Partner shall, with support from the Authority, develop the DSA System Design. The DSA System Design shall meet the requirements as set out in the DSA SRD and the DSA System Architecture and shall be baselined at the Formal Design Reviews (detailed at para 61 below).
16. The DSA System Design documentation shall include but shall not be limited to:
17. System use cases - to support specification and requirement traceability.
18. Subsystem Requirements Documents (SSRDs)/Technical Product Specifications for radio and components.
19. Interface Control Documents.
20. Supporting technical drawings/diagrams.
21. System constraint information.
22. Design decisions.
23. Draft Bill of Materials, for both software and hardware system components. This Bill of Materials shall be further developed collaboratively between the Authority, Design and Integration Partner and the Authority's third-party suppliers (where applicable).
24. Rough Order of Magnitude (ROM) costs.
25. All design documentation produced by the Design and Integration Partner shall be clear and comprehensive, in a format to be agreed between both parties. All design documentation shall be subject to a rigorous review processes which shall include the Authority and relevant third parties (where appropriate).
26. The Design and Integration Partner shall, with agreement from the Authority, baseline the DSA System Design at the appropriate Formal Design Reviews and manage the baselines in line with the process detailed at para 73 below.
27. The Authority shall have full ownership rights for all design documentation and deliverables detailed under this Statement of Requirement. The Authority shall use any or all design documentation and/or deliverables developed under this Statement of Requirement to contract its third-party suppliers (including for use in the Authority's competition process). The Authority shall provide design documentation and/or deliverables to other projects/programmes/third parties for future interfacing to/with (as appropriate).
28. **Design Requirements, Principles and Considerations for the DSA System Design.** The following paragraphs detail the requirements, principles and considerations for the Design and Integration Partner to incorporate into the DSA System Design:
29. The DSA System Design produced by the Design and Integration Partner shall be modular, use widely supported standards for its key interfaces, and be subjected to successful verification and validation tests to ensure the openness of its key interfaces.
30. **Openness –** To enable better management of obsolescence and prevent "Vendor Lock In", the Design and Integration Partner shall adopt an open system design. This shall deliver the following benefits:
31. Ease of interoperability between systems, sub-systems and components.
32. The ability to modify the capability for different operational roles.
33. Support potential reuse of common Off-The-Shelf (OTS) and open source-based equipment and software.
34. Improve integration.
35. Support technology refresh, obsolescence management and capability insertion and ensure that the system can evolve through life.
36. **GFA offered by the Authority:** The Design and Integration Partner shall consider the potential for use of any equipment/components/software offered by the Authority on a GFA basis and shall incorporate any GFA found to be beneficial into the DSA System Design. If any GFA offered by the Authority is rejected by the Design and Integration Partner, it shall be confirmed with the Authority in the next appropriate Design Review.
37. **Electromagnetic Integration Management:** Electromagnetic Environmental Effects (E3) is the term given to all disciplines relating to electromagnetic phenomena e.g. Electromagnetic Compatibility (EMC), Mutual Interference (MI), Radiation Hazard (RadHaz) and TEMPEST etc.
38. The Design and Integration Partner shall, with support from the Authority, be responsible for the provision of E3 documentation and evidence laid out in the BATCIS E3 Requirements and Management Policy (RAMP) [reference Q] available at Contract Award. This may include the provision of EMC, MI, RadHaz or TEMPEST testing.
39. The Design and Integration Partner shall produce the following documents to ensure compliance with the BATCIS E3 RAMP where applicable, and where agreed with the Authority:
40. E3 equipment certification specifications.
41. Technical drawings and/or models.
42. E3 Test Plans.
43. Test Readiness Review Output Documents.
44. E3 Test Reports.
45. **Human Factors Integration (HFI):** The Design and Integration Partner shall plan and implement Human Factors Integration activities to support the definition, design, specification and evaluation of the system and its component products to support all user roles to achieve their goals effectively, safely, with the minimum of training burden and with optimal levels of physical task load and cognitive burden. To this end, the Design and Integration Partner shall ensure the HFI activities are conducted by suitably qualified and experienced HFI subject matter experts. The Design and Integration Partner shall provide HFI reports as agreed between both parties.
46. **Operational Service Management:** The Design and Integration Partner shall design for Operational Service Management. This is utilisation of quality IT services that meet the need of the Operating Authority, performed through a mix of organisations and people, value streams and processes, information technology and tools, partners and suppliers. The Design and Integration Partner shall design in accordance with, and align to the following:
47. Mission Services Assurance Approach to LE TacCIS [reference R], available at Contract Award.
48. KiD guidance:
49. Software requirements including direction on contracting for software support, SRD and URDs [reference S].
50. Generic software support requirements [reference T].
51. Software Support Plans [reference U] and other required documentation.
52. The IT Infrastructure Library (ITIL) Framework Service Management Strategy, V4 [reference V].
53. The Defence Digital Operations Head Quarters Operational Service Management Context Document [reference W], available at Contract Award.
54. The Design and Integration Partner shall evolve and adapt the DSA System Design in response to capability roadmaps, technology innovation, emerging user needs, system or technical vulnerabilities and/or system obsolescence.
55. **Formal Design Reviews**[[19]](#footnote-20)**:** Formal Design Reviews shall take place to review and agree the documentation provided to date and to authorise commencement to the next stage of development. The Design and Integration Partner shall support these reviews through production of required evidence/deliverables/technical information and attendance. It is anticipated that the Formal Design Reviews detailed at para's 61a-e below shall take place (as a minimum). This shall be agreed between the Authority and the Design and Integration Partner at Contract Award.
    1. **System Requirements Review (SRR):**
56. **Purpose:** To ensure that the preliminary system requirements are traceable to the user requirements and are sufficiently detailed and understood to enable a system functional definition and architectural description to be derived that meet system performance specifications.
57. **Timing:** Expected to be held within 3 months of Contract Award.
58. **Input:** Updated SRD.
59. **Output:** Agreed SRD baseline.
    1. **Preliminary Design Review (PDR**):
60. **Purpose:** Multi-disciplined product and process assessment to ensure that the proposed DSA System Design under review can proceed into detailed design, meet the stated performance requirements in the SRD and fulfil the DSA Concept of Employment [reference X] (available at Contract Award), within the approved performance, cost, time parameters and risk constraints.
61. **Timing:** This shall occur prior to the Radio Provider competition and is expected to take place within 6 months of Contract Award.
62. **Inputs:** Updated SRD, updated DSA System Architecture, DSA System Design and supporting design deliverables (see Annex A), SSRD and technical product specifications, proposed Developmental DSA System, proposed DSA Public Key Infrastructure (PKI) System Design and supporting deliverables (see Annex A), proposed development and support tools.
63. **Outputs:** Agreed SRD, agreed DSA System Architecture, agreed DSA System Design and supporting design deliverables, agreed SSRD and technical product specifications, agreed Developmental DSA System, agreed DSA PKI System Design and supporting deliverables, agreed development and support tools.
    1. **Radio Subsystem Design Review (RSDR)**:
64. **Purpose:** Multi-disciplined product assessment to ensure that the proposed radio subsystem requirements documents and technical product specifications meet the stated performance requirements in the DSA SRD and fulfils the Concept of Employment within the approved performance, cost, time parameters and risk constraints.
65. **Timing:** This shall occur prior to the Radio Provider competition and is expected to take place within 6 months of Contract Award (may be combined with or separate to the PDR above).
66. **Inputs:** Radio SSRD and technical product specification.
67. **Outputs:** Agreed Radio SSRD and technical product specification.
    1. **Interim Design Reviews (IDRs**):
68. **Purpose:** Multi-disciplined product and process assessment to ensure that the proposed detailed solution design under review incrementally matures towards the System Design Review (see para 61e below).
69. **Timing:** Expected to be held every 6 months after the Preliminary Design Review (detailed at para 61b above) up to the System Design Review ((see para 61e below), i.e. months 12 and 18).
70. **Inputs:** Updated SRD, updated DSA System Architecture, updated DSA System Design and supporting design deliverables (see Annex A), updated SSRDs and technical product specifications, updated Developmental DSA System, updated DSA PKI System Design and supporting deliverables (see Annex A), updated development and support tools.
71. **Outputs:** Agreed SRD, agreed DSA System Architecture, agreed DSA System Design and supporting design deliverables, agreed SSRDs and technical product specifications, agreed Developmental DSA System, agreed DSA PKI System Design and supporting deliverables, agreed development and support tools.
    1. **System Design Review (SDR):**
72. **Purpose:** This review ensures that the DSA System Design can effectively support the FBC submission. The review must consider the preferred bidder solution for the radio and the proposed solution for the system components. The review shall:
73. Identify the impact of any trade-offs, compromises or expectations required against the requirements.
74. Ensure that the boundary, interface and interoperability issues and risks are understood, clearly documented and managed.
75. Address legacy constraints, dependencies and engineering speciality requirements.
76. **Timing:** Expected to take place within 24 months of Contract Award
77. **Inputs:** Updated DSA System Architecture, updated SRD, updated DSA System Design and supporting design deliverables (see Annex A), updated SSRDs and technical product specifications, final Developmental DSA System, final DSA PKI System Design and supporting deliverables (see Annex A), proposed System Integration Test Report.
78. **Outputs:** Agreed DSA System Architecture, agreed SRD, agreed DSA System Design and supporting design deliverables, agreed SSRDs and technical product specifications, accepted final Developmental DSA System, agreed final DSA PKI System Design and supporting deliverables, agreed System Integration Test Report.
79. **Management of Formal Design Reviews**. As detailed at para 61 above, the Design and Integration Partner shall be required to attend and contribute to a set of Formal Design Reviews which shall be chaired by the Authority. The conduct of the formal/major design review meetings shall be as follows:
80. All documentation shall be made available to the Authority and appropriate stakeholders no later than 15 working days prior to each planned review meeting.
81. Stakeholders required to review the Design and Integration Partner documents shall be selected and notified by the Authority. All stakeholders shall review the documentation prior to the review meeting.
82. The Design and Integration Partner shall organise, coordinate and support each review meeting and present the findings in a suitable medium to the Authority (medium to be decided between the Design and Integration Partner and the Authority).
83. During the review meeting, the Design and Integration Partner shall record the meeting actions and decisions against the presented content and provide detail of the significant issues within documents addressed. Actions are to be agreed at close of the review meeting. Actions and decisions shall be issued to the Authority within 5 working days of the meeting.
84. The satisfactory acceptance of the review meeting shall be approved by the Authority upon the successful closure of agreed actions.
85. **Continuous Assurance Activities:** Additional informal developmental design reviews and meetings shall take place (as required) and shall be managed on an informal collaborative working basis; i.e. slide packs produced and issued the day before the meeting, records of actions shared on the Authority's shared working environment etc. This may include sub-system readiness reviews (if required) prior to and in preparation for Formal Design Reviews. Due to the delaminated procurement approach, it is anticipated that some design reviews shall be multi-vendor and the Design and Integration Partner shall be required to work collaboratively with the Authority and their suppliers in advance of and post review.
86. **Shared Working Environment - Technical Library:** The Design and Integration Partner shall support the Authority with the creation of a shared Technical Library, hosted on the Authority's shared working environment. The Design and Integration Partner shall support the Authority in the identification, sourcing and maintenance of the necessary standards, policy, principles and guidelines required for the delivery of this contract[[20]](#footnote-21). A monthly review of the shared Technical Library shall be conducted by the Authority and the Design and Integration Partner, to ensure accuracy and continued alignment between both parties.
87. **Design Repository (within the Technical Library):** The Design and Integration Partner shall support the Authority in the development of a design repository structure (within the Technical Library) to hold all design and system integration documentation and software. The Design and Integration Partner shall support the Authority in the implementation and management of the design repository, including:
88. File storage and information exchange process for the Authority, the Design and Integration Partner, and third-party supplier artefacts and software.
89. Document configuration, change and action management tooling, to include the following capabilities:
90. Perform fully traceable document reviews and approval cycles.
91. Create actions in association to documents.
92. Document configuration changes with folder-based security access.
93. Formal repository, records and inventory database.
94. Customisable document metadata in accordance with the needs of a project or mission.
95. Ability to automate the creation of document reference numbers according to specific project or Authority departmental rules.
96. Dynamic search and export capability.
97. Multiple Author response tracking.
98. Audits.
99. Report generation.
100. Inability to remove files or folders to ensure that historical documentation is retained.
101. **Proactive Future Technology and Obsolescence Management.** The Design and Integration Partner shall proactively manage the obsolescence of the DSA System and produce the following documents, to inform the Authority of the future technology and obsolescence issues affecting the DSA capability:
102. **Technology Horizon Management Roadmap**, demonstrating evolution options for the capability at agreed intervals. Technology Horizon Management identifies, evaluates, and prioritises activities to exploit new technology. The Design and Integration Partner shall conduct horizon scanning and maintain a technology roadmap to identify intervention opportunities driven by changes in technology or changing/emerging User requirements. The Design and Integration Partner shall provide a Technology Horizon Management Roadmap within 6 months of Contract Award; this shall be updated as a minimum on a 6-monthly frequency or upon identification of a new technology (whichever is sooner).
103. **Obsolescence Management Plan**, which demonstrates the Obsolescence Management processes, responsibilities, resources and procedures required to identify, analyse, manage, review, treat and resolve obsolescence risk and issues across the DSA project lifecycle. The Design and Integration Partner shall liaise with the Authority to ensure Obsolescence Management Plans and mitigation/resolution of obsolescence issues are appropriately aligned with the Authority’s ECD Programme. The Obsolescence Management Plan shall be provided to the Authority within 6 months of Contract Award; this shall be updated as a minimum on a 6-monthly frequency or upon identification an obsolescence issue (whichever is sooner). The Design and Integration Partner shall carry out the activities detailed within the Obsolescence Management Plan.
104. **Obsolescence Roadmap**: The Design and Integration Partner shall work with the Authority and its third-party suppliers to develop an Obsolescence Roadmap. The Design and Integration Partner shall use International Electrotechnical Commission (IEC) 62402:2019 (Obsolescence Management) [reference Y] in the development of the Obsolescence Management Plan and Obsolescence Roadmap. The Obsolescence Roadmap shall be provided to the Authority within 6 months of Contract Award; this shall be updated as a minimum on a 6-monthly frequency or upon identification an obsolescence issue (whichever is sooner). Any configuration changes due to obsolescence shall be approved in accordance with the Configuration Management process defined in this Statement of Requirements (para 73b below). The Design and Integration Partner shall provide the Authority with obsolescence status updates, as part of the periodic project meetings.
105. **Engineering Management Plan:** The Design and Integration Partner shall develop an Engineering Management Plan, which shall comply with/follow MOD standards, policy, principles and guidelines (as well as industry best practise). The Engineering Management Plan shall be delivered within 2 months of Contract Award and shall be made available to the Authority's third-party suppliers and stakeholders, for acknowledgment and alignment (where required). The Design and Integration Partner shall implement and carry out the activities within this plan.
106. The Engineering Management Plan shall be sub-ordinate to the Authority’s System Engineering Management Plan [reference Z] (available at Contract Award). Both parties shall work collaboratively to further develop these documents, ensuring alignment throughout.
107. **Support to Authority Working Groups:** The Design and Integration Partner shall support and attend nominated Working Groups, including but not limited to design, training, integrated logistics support, security, safety, requirements, capability integration working groups.
108. The above processes and ways of working shall be subject to amendment as the collaborative relationship between the Authority and the Design and Integration Partner develops, and improvements to the processes, procedures and way of working are identified, agreed and adapted by both parties during delivery of the contract.

003 - SUPPORT TO AUTHORITY COMPETITIONS

1. The Design and Integration partner shall support the Authority with the production of documentation and technical work packages associated with the radio procurement, which shall include (but shall not be limited to) the design documentation already detailed within section 002 of this document and additional Statements of Work (as required).
2. **Support to Radio Provider Competition Process:** The Design and Integration Partner shall support the Authority in its competition activity for the Radio Provider and down-select trials. This shall include support to preparation for the competition, support to the evaluation process and support to the radio down-select trials, as detailed below.
3. The Design and Integration Partner shall provide support to the following competition activity:
4. **Contract Notice/Dynamic Pre-Qualification Questionnaire (DPQQ) Stage**: Input to Contract Notice; Input to DPQQ and DPQQ evaluation strategy (including attendance at multiple workshops); Support Authority responses to clarification questions; Conduct DPQQ evaluation; Attend moderation of DPQQ evaluation; Support to Authority preparation of debrief letters.
5. **Tender Stage (which may include but may not be limited to):** Support to development of Statement of Requirement (including attendance at multiple workshops); Completion of Authority funded AWARD[[21]](#footnote-22) training; Support to production of supporting documentation; Support to production of Evaluation Strategy (including attendance at multiple workshops); Support to production of Negotiation Strategy (as applicable) (including attendance at multiple workshops); Support to production of Contract Terms and Conditions; Support Authority responses to clarification questions; Conduct Tender Evaluations; Attend moderation of Tender Evaluations; Support down select radio demonstrations and trials; Conduct lab based evaluations; Support the Authority with preparation for negotiations; Support negotiations (multiple workshops/meetings with each supplier); Conduct Best And Final Offer (BAFO) evaluations; Attend moderation of BAFO evaluations; Support to Authority preparation of debrief letters.
6. The above processes and ways of working shall be subject to amendment as the collaborative relationship between the Authority and the Design and Integration Partner develops, and improvements to the processes, procedures and way of working are identified, agreed and adapted by both parties during delivery of the contract.

004 - MANAGE CHANGE CONTROL & CONFIGURATION MANAGEMENT

1. Change Control and Configuration Management activities shall be carried out in accordance with the Authority's agreed processes and procedures, set out in the following paragraphs:
2. **Project Change Control:** When a change is identified against a baseline, by either the Authority or the Design and Integration Partner, the following change process shall be followed:
3. A Change Request Form shall be raised by the party who identifies the change (template to be provided by the Authority).
4. The Authority shall log the change request in the project master change register and send a request for impact assessment to the Design and Integration Partner (and any other parties involved in the change).
5. The Design and Integration Partner (and any other parties involved in the change) shall provide the impact information (including the associated Performance, Cost and Time (PCT) impacts to affect the change).
6. The Authority shall conduct an impact and validity assessment of the change and review proposed PCT impact against project budget, project milestones and project requirements and outputs. If the change is deemed valid it shall be submitted to the Change Control Board for approval. If deemed invalid, the change shall be recorded as closed on the change register and no further action taken.
7. The Change Control Board shall either approve or reject the change. In the event that the change is rejected, the change shall be recorded as closed on the change register and no further action shall be taken. In the event that the change is approved, the Design and Integration Partner and Authority shall develop a Joint Implementation Plan which shall be agreed between both parties.
8. In the event that the change is approved and results in the requirement for a formal change to the contract, the parties shall refer to Clause 24 of the DOS 5 Framework Core Terms [reference AA] and the Authority shall complete the Variation Form (Joint Schedule 2 of the DOS 5 Framework) [reference BB], to initiate a formal contract change.
9. Upon acceptance of the contract change, all parties shall implement the change, communicate the change to their relevant parties and the Authority shall update the Project Change Register.
10. **Configuration Management:** The following process shall be followed for project configuration management:
11. As the subject matter expert in configuration management, the Design and Integration Partner shall support the Authority in the production of a Configuration Management Plan, applicable to both project and technical configuration management, feeding in best practise and ways of working.
12. Both parties shall work together to identify and agree Configuration Management Items/Artefacts (including those provided by third parties), which shall be subject to configuration control. The Authority shall update the Configuration Management Item/Artefact Baseline Repository (which shall be held on the Authority's shared working environment) with the agreed Configuration Management Items/Artefacts.
13. The Authority and Design and Integration Partner shall store, maintain and manage all Configuration Management Items/Artefacts on the Authority's shared working environment. The Authority shall update and maintain the Configuration Management Item/Artefact Baseline Repository.
14. For Configuration Management Items/Artefacts subject to change control, the change control process at para 73a shall apply.
15. Any Items/Artefacts not subject to configuration control shall be managed and maintained on the owner's (Authority, Design and Integration Partner, or third-parties') own item/artefact (storage) systems.
16. **Baseline Reference Management:** The Design and Integration Partner shall manage baseline reference material including DSA system baseline(s) to facilitate the management of change, testing and validation of new builds, configuration items and software patches/updates.
17. The Design and Integration Partner shall develop a Baseline Reference Management Plan and set up a Baseline Reference Material Repository as detailed within the Plan, within 6 months of Contract Award, which shall hold baseline reference material for all releases and deployed configurations. It shall be a shared repository accessible by the Authority and its third-party suppliers.
18. A baseline reference set/centre shall be maintained by the Design and Integration Partner and held at their premises (unless otherwise agreed with the Authority).
19. The Design and Integration Partner shall develop and populate the Initial Baseline Reference Material and baseline the Configuration Model throughout the assessment phase.
20. The Design and Integration Partner shall maintain and control the configuration of the DSA System Architecture, DSA System Design and technical baselines on behalf of the Authority, ensuring on-going system openness. This shall be reported and reviewed at the Change Boards as detailed in the Change Control and Configuration Management Process listed above.
21. The above processes and ways of working shall be subject to amendment as the collaborative relationship between the Authority and the Design and Integration Partner develops, and improvements to the processes, procedures and way of working are identified, agreed and adapted by both parties during delivery of the contract.

005 - MANAGE SYSTEM INTEGRATION

1. The Design and Integration Partner shall be responsible for all aspects of system integration, for the duration of the contract, including the approach to system integration, the implementation of system integration and achievement of the overall outcome of system integration.
2. **Integrated Test, Evaluation and Acceptance Plan (ITEAP).** The Design and Integration Partner shall review the DSA Integrated Test, Evaluation and Acceptance Plan [reference CC] provided by the Authority (at Contract Award) and support the Authority in conducting evaluation and acceptance activities as part of the design review process.
3. **Developmental DSA System.** The Design and Integration Partner shall procure small scale components and build a Developmental DSA system, to prove the maturity of the DSA System Design. This Developmental DSA system shall be provided at PDR and updated throughout the design process with a final Developmental DSA System presented at SDR.
4. **Integration:** The Design and Integration partner shall:
   1. Present the DSA System Design and Developmental DSA System at the appropriate Formal Design Reviews (see para 61 above).
   2. Provide or arrange their own access to a suitable configurable testing environment.
   3. Conduct integration evidence gathering activities.
   4. Conduct simulated proof of system design activities on the Developmental DSA system.
   5. Conduct testing of the Developmental DSA System in accordance with the DSA ITEAP:
5. Integration testing (plans, scripts, testing & reports).
6. Regression testing (plans, scripts, testing & reports).
7. System integration testing (plans, scripts, testing & reports).
8. Specialist testing e.g. security.
9. **DSA Design Conformance**: The Design and Integration Partner, with support from the Authority, shall be responsible for physical conformance testing. Conformance testing shall include all activities and documentation required to prove and accept the DSA System Design.
10. The Design and Integration Partner shall manage and publish a test schedule on the Authority's shared working environment and the Authority shall witness testing as required.
11. **System Verification**: The Design and Integration Partner shall support the Authority with the management of verification and validation activities and provide the required evidence[[22]](#footnote-23) (as required). The Design and Integration Partner shall produce an overarching System Integration Test Report, which shall be used on the Developmental DSA system (and for the Authority to use on its production system). This shall be an input to the SDR.
12. Where possible the Authority shall use progressive verification to give confidence that the DSA Developmental System is operationally stable, meets all the requirements and could be subsequently deployed.
13. The Authority reserves the right to conduct third party testing/assurance of the developmental DSA system.
14. The Design and Integration Partner shall support the Authority with any and all third-party testing/assurance activities.
15. **Integration Assurance:** The Design and Integration Partner shall carry out its own Integration Assurance process and shall support the Authority's assurance activities on the Developmental DSA System.
16. The above processes and ways of working shall be subject to amendment as the collaborative relationship between the Authority and the Design and Integration Partner develops, and improvements to the processes, procedures and way of working are identified, agreed and adapted by both parties during delivery of the contract.

006 - SYSTEM DESIGN AUTHORITY (SDA), SYSTEM SAFETY & SYSTEM SECURITY

1. The Design and Integration Partner shall be responsible for SDA governance, including development and management of SDA processes/procedures, with the Authority retaining the overarching assurance role. Whilst the relationship shall be subject to a collaborative decision-making process, the Authority reserves the right to override or have the final say on decisions that affect the interests of the DSA project. This shall apply to all sections of this document.
2. **System Design Authority requirements and responsibilities:** The Design and Integration Partner shall be responsible for the providing technical oversight and establishing the appropriate governance frameworks for the DSA system. For clarity and completeness, the full list of SDA responsibilities has been included below:
3. Requirements and Specifications:
4. Analysis of customer requirements.
5. Specifying system and subsystem requirements.
6. Developing system and subsystem specifications.
7. Defining engineering work packages and sub-design specifications.
8. Architecture and Design - development and management:
9. DSA System Architecture definition.
10. DSA System Design definition.
11. Internal and external interface definition;
12. Technical Governance:
13. Develop/refine effective value adding, tailorable design governance framework.
14. Review and approve project tailoring of governance framework based on applicability.
15. Manage interface with other governing bodies (where applicable).
16. Support to audits by applicable organisations (where applicable).
17. Provide information to the Authority to allow technical decision making.
18. Support to technical governance of Authority suppliers (where applicable).
19. Support upkeep of the Technical Library and Design Repository, with reference to applicable architectural & integration standards transcribed in the programme context and reflected in programme level architectural artefacts.
20. Production of best practise technical artefact templates & examples.
21. Planning, development and control of technical configurations & baselines.
22. Management of change to technical baselines throughout the project lifecycle.
23. Test and Acceptance.
24. Technical Assurance:
25. Of engineering outputs, including engineering plans, test plans, detailed designs, interface specifications, qualification evidence and third-party supplier equipment.
26. Structure technically focussed evaluations (e.g. make/buy analysis) objectively around clear criteria linked to business goals, value and outcomes.
27. Presentation of results such that effective decisions can be made by the Authority stakeholders.
28. Technical Risk:
29. Support the Authority in identification and management of technical risks, mitigation strategies & alternative approaches with costings through a structured scenario and consequence-based approach.
30. Support the Authority in identification and management of Safety and Security risks/hazards, mitigation strategies & alternative approaches with costings through a structured scenario and consequence-based approach.
31. Develop technical roadmaps aligned to capability roadmaps to enable technical change to be planned and delivered at the most effective block points.
32. Technology planning & management to identify & develop promising low Technology Readiness Level technologies to support planned capability increments.
33. **System Safety and Environmental Management:** The Design and Integration Partner shall plan and implement safety and environmental management actions aimed to ensure the development of products, services or systems which are safe and environmentally sound. This shall be articulated in the Design and Integration Partner DSA Safety and Environmental Management Plan and supplied to the Authority at Contract Award.
34. The Design and Integration Partner shall provide a robust safety and environmental argument for the DSA system through hazard identification, hazard analysis, risk assessment and risk classification using the criteria detailed in the DSA System Part 1 - Safety and Environmental Case Report [reference DD] issued at Contract Award. The Design and Integration Partner shall produce the Part 2 (Design) Safety Case Report and supporting hazard log, analysis and evidence within 12 months of Contract Award and provide safety assurance ensuring compliance with MOD, Defence Digital & BATCIS Policy, at key project intervals providing the safety management status of the system design.
35. The Design and Integration Partner shall ensure compliance/alignment with the following Safety Standards/Regulations and DSA Documents:
36. Safety Standard DEFSTAN 00-056 - Safety Management Requirements for Defence Systems [reference EE] and DEFSTAN 00-051 - Environmental Management Requirements for Defence Systems - Requirements [reference FF].
37. Safety Standard DEFSTAN 00-055 - Requirements for Safety of Programmable Elements (PE) in Defence Systems [reference GG] (for System Functional Safety implemented via Software, Hardware and Firmware).
38. Safety and Environmental Regulation DSA02 [reference HH] (available at Contract Award).
39. Safety and Environmental Regulation DSA03 [reference II] (available at Contract Award).
40. DSA System Part 1 - Safety and Environmental Case Report (available at Contract Award).
41. DSA System Safety and Environmental Management Plan [reference JJ] (available at Contract Award).
42. The Design and Integration Partner shall manage and maintain their own Safety and Environmental Management System (SEMS), which may be subsumed into the Safety and Environmental Management Plan (S&EMP) and conduct safety management activities in line with these. These shall be provided by the Design and Integration Partner at Contract Award.
43. The Design and Integration Partner shall provide support to Authority requested safety meetings, including safety meetings with the Authority's third-party suppliers.
44. The Design and Integration Partner may be subjected to periodic Safety and Environmental Audits (no more than 1 per annum) and be expected to provide the evidence and artefacts to support any safety or environmental claims in addition to oversight of the management of their internal Safety and environmental management system. The Authority shall provide the Design and Integration Partner with notice, in writing, of any impending Safety and Environmental Audits.
45. **Security Management, Assurance, Risk Management and Accreditation:** At Contract Award, the Design and Integration Partner shall appoint a Security point of contact to act as the liaison between the Authority Security Manager and the Design and Integration Partner. Post Contract Award, and within 1 month of Contract Award, the Design and Integration Partner shall be required to produce the following artefact to support the Design and Integration Partner elements of Security Management:
    1. **Design and Integration Partner Security Management Plan (SMP):** The Design and Integration Partner SMP shall be a subordinate of the Authority's SMP [reference KK] (available at Contract Award) and shall cover how the Design and Integration Partner shall manage their responsibilities to Security Management, Security Assurance, Security Risk Management and Security Accreditation. A product description for the Supplier SMP will be provided at Contract Award [reference LL] to assist with the production of the SMP and guide content inclusion. The Design and Integration Partner SMP shall cover the entire breadth of their delivery. The following Artefacts shall be required to be produced by the Design and Integration Partner during their tenure. The frequency of delivery of these artefacts shall depend upon how the Design and Integration Partner design their delivery strategy however the Authority believe that the requirement shall be at least once, with updates made to a single artefact as the project develops. The Authority considers that living documents with robust version control are preferable to multiple documents:
46. Security Assurance Case Reports (Assurance Evidence).
47. Security Impact Assessments.
48. Security Cases.
49. Design and Integration Partner Meeting Requests and Minutes/Record of Actions and Decisions (ROADs).
50. DSA Security Operating Procedures (minimum of user and privileged user).
51. Design and Integration Partner Security Input to Test Plans.
52. The Design and Integration Partner shall be responsible for its own adherence to any regulations put in place as part of the Contract Award i.e. adherence to Industry Security Notices, Contract Security Aspects Letters, Defence Standards etc. To that end, the Authority considers the Design and Integration Partner responsible for the following, and the DSA Accreditor/DSA Security Manager shall not hold responsibility for the accreditation and management of Design and Integration Partner infrastructure or the sub-contracting elements of Supply Chain Security, however will require evidence to be provided as to the supplier’s adherence to Commercial and Supply Chain Security Standards:
53. Design and Integration Partner owned Infrastructure Accreditation Artefacts and Management.
54. Supply Chain Security and Assurance Compliance Artefacts.
55. The Design and Integration Partner shall be required to work collaboratively with the Authority on the production of Accreditation, Security Assurance and Risk Management artefacts that support the Accreditation and delivery of a secure and compliant DSA system. The full list of these Accreditation, Security Assurance and Risk Management artefacts [reference MM] shall be provided by the Authority at Contract Award; however the list contains collaborative requirements for the DSA Accreditation Evidence Statement, and the Design and Integration Partner input shall include factual information and Design Collateral to help build the Accreditation Case. The Authority shall remain responsible for the Accreditation with the Design and Integration Partner as a key stakeholder in designing a secure DSA and providing Assurance Evidence to the Authority. The Authority shall remain responsible for Accreditor/Cyber Defence and Risk team engagement however the Design and Integration Partner shall be required to attend Assurance meetings at the request of the Accreditation Authority on an ad-hoc basis. The Authority shall remain responsible for the delivery and production of the following artefacts:
56. Authority Security Management Plan.
57. DSA Accreditation Strategy [reference NN] (available at Contract Award).
58. Accreditation Evidence Statement [reference OO] (available at Contract Award).
59. Security Aspects Letters - Radio Provider [reference PP] (not yet developed).
60. Snapshot Technical Risk Assessment [reference QQ] (available at Contract Award).
61. In-House Threat Assessment [reference RR] (available at Contract Award).
62. Security Risk Register [reference SS] (available at Contract Award).
63. Risk Treatment Plan [reference TT] (available at Contract Award).
64. The Design and Integration Partner shall provide support to the Authority in the development of the following products and/or provide the Authority with the support to completion of the following activities:
65. DSA Technical Risk Assessment.
66. DSA/BATCIS Coordinating Design Organisation (CDO) Security Risk Register.
67. DSA Project Crypto Plan.
68. DSA Risk Management and Accreditation Document Sets (RMADS).
69. DSA Baseline Control Set.
70. DSA Accreditation Scoping Appraisal.
71. DSA Risk Treatment Plan.
72. National Cyber Security Centre Cloud Security Compliance Statement.
73. Information Security Management Plan.
74. DSA Security Working Group (SWG) ROADs.
75. DSA Anti-Virus (AV) Policy.
76. DSA Digital Forensics Policy.

m. DSA Protective Monitoring Policy.

n. DSA Incident Management Policy.

1. DSA Patching Policy.
2. Information Technology Health Checks (ITHC) Scoping Documents.
3. ITHC Remediation Plans.
4. ITHC Remediation Tracker.
5. Vulnerability Assessments.
6. DSA Security Impact Assessments.
7. DSA Business Continuity Plan.
8. DSA Data Management Plan.
9. DSA Authority to Test Management Plan.
10. DSA Risk Balanced Cases.
11. DSA Security Grading Guide.
12. Security Assurance Case Report.
13. SWG Minutes.
14. As a minimum, the Design and Integration Partner shall be required to attend and support the following meetings at the frequency stated:
15. SWG: Quarterly.
16. DSA Security Meeting: Bi-Monthly.
17. DSA Security Risk Reviews: Monthly.
18. The Design and Integration Partner shall comply with the guidance and direction in the following Security Frameworks/Standards/Policies as a minimum:
19. CDO External Governance Requirements [reference UU] (to be advised by the Authority as required).
20. MOD Internal Policy and Governance [reference VV] (available at Contract Award).
21. Her Majesty's Government (HMG) - Good Practice Guides [reference WW] (to be advised by the Authority as required).
22. HMG - Security Policy Framework [reference XX].
23. HMG - Information Assurance Standard (IAS) I&2 [reference YY].
24. British Standards European Norm (BS EN) International Organization for Standardization (ISO) 27001/2-2017 - Information technology — Security Techniques — Information Security Management Systems — Requirements [reference ZZ].
25. CDO Security Assurance Framework [reference AAA] (available at Contract Award).
26. Additional Security Assurance Evidence (as required).
27. **Public Key Infrastructure (PKI):** Within 6 months of Contract Award (for PDR), the Design and Integration Partner shall develop a DSA PKI System Design[[23]](#footnote-24). The Design and Integration Partner shall:
28. Collaborate with Authority and its third-party suppliers/stakeholders in context of the DSA SWG.
29. Develop DSA PKI System Design Specifications – including Operational Security Governance, Processes and Procedures and Key Management Plan in line with the Authority PKI approved system design.
30. Procure, install, set up & test DSA Standalone PKI on the developmental DSA system in line with the system designs and ITEAP – including:
31. Offline Certification Authority (CA) root.
32. Registration Authority (RA) i.e. subordinate CA.
33. X509 Certificate Database and Store.
34. Key Archival Server.
35. Key Management Trust Anchors (KMTA) and Ops Keys for radios and end user device.
36. Develop DSA PKI configuration data and test logs.
37. Work collaboratively with the Authority and its third-party suppliers to develop and understand Test ITEAP for KMTA & Operational Keys.
38. Support the Authority with User Acceptance activities (if required).
39. Through close collaboration with the Authority, the Design and Integration Partner shall ensure that the overall design for operational service management shall include operational DSA PKI Operations, including Key ordering service as well as the following:
40. Crypto Custodian.
41. Identity & Access Management (IDAM) services for DSA users and devices.
42. Key management services for certificates for Identity, Integrity, Confidentiality & non-repudiation.
43. PKI Audit & Monitoring services.
44. Event & Incident management services.
45. Certificate Revocation services.
46. Disaster Recovery (DR) services.
47. Secure Key Disposal services.
48. The Design and Integration Partner shall enable DSA PKI Operational Support Options for specific Tactical/Deployed missions, including but not limited to:
49. Deployed subordinate CA option.
50. Mission embedded DSA Crypto Custodian.
51. The Design and Integration Partner shall maintain the DSA PKI Audit Database, event logs & Service Level Agreement (SLA) evidence (if applicable) and feed back into the Authority Crypto Controller/PKI Crypto Management as and when required to.
52. The above processes and ways of working shall be subject to amendment as the collaborative relationship between the Authority and the Design and Integration Partner develops, and improvements to the processes, procedures and way of working are identified, agreed and adapted by both parties during delivery of the contract.

007 - ADDITIONAL AD-HOC TASKING

1. The Design and Integration Partner shall carry out additional ad-hoc taskings as agreed between the Authority and the Design and Integration Partner, in accordance with the tasking procedure detailed in the contract.

008 - SUPPORT TO TRAINING, INTRODUCTION TO SERVICE & LOGISTICS SUPPORT

1. **Development and Support Tools:** The Design and Integration Partner shall be responsible for providing the tooling required to support the development of (and design for subsequent in-service support of) the DSA system. This shall be provided as an input to the PDR. The Design and Integration Partner shall provide documentation on use and appropriate Training Material on tooling. The tooling shall be able to:
2. Create, amend and support applications, programs and utilities to enable the Authority to build and iterate the DSA system.
3. Allow integration with other Authority software development tools.
4. Debug and analyse system for robustness, maintainability and security.
5. **Software Supportability:** The Design and Integration Partner shall be responsible for development of the Software Support Plan (which shall feed into the Authority's Integrated Logistics Support Plan [reference BBB] (available at Contract Award)). The Software Support Plan shall be provided within 12 months of Contract Award. The Design and Integration Partner shall be responsible for development of the following deliverables in support of this requirement:
6. Test Plans: Acceptance, System Integration, Regression.
7. System Integration Readiness Review Minutes.
8. Acceptance Test Readiness Review Minutes.
9. Acceptance Test Scripts.
10. Acceptance Test Reports.
11. Regression Test Report.
12. Regression Test Scripts.
13. System Integration Test Scripts.
14. System Integration Report.
15. Release Certificate.
16. **Licence Management:** The Design and Integration Partner shall provide a perpetual licence agreement with general deliverable user rights, without limitation to copy, modify, disclose and use by the Authority and its appointed subcontractors for any proprietary software developed during the contract.
17. **Support to Technical Publications:** To enable the Authority to meet its legal duty of care obligations, it is a requirement that the Design and Integration Partner shall deliver Technical Information to ensure the safe integration, operation, maintenance, repair, support and disposal of a Platform, System, or Equipment (PSE) throughout its life. The Design and Integration Partner shall provide support and information (as requested by the Authority) to the Authority to produce the required DSA Technical Publications [reference CCC] (not yet developed). The Design and Integration Partner shall review and comment on the Authority produced Technical Publications (as and when requested to do so by the Authority).
18. **Integrated Logistics Support:** The Design and Integration Partner shall develop an Integrated Support Plan that aligns with the Authority’s Integrated Logistics Support Plan which shall be available at Contract Award. Upon acceptance of the Integrated Support Plan by the Authority, the Design and Integration Partner shall deliver the activities and services within the scope of the Integrated Support Plan. The Integrated Support Plan shall be delivered within 12 months of Contract Award.
19. **DSA Training Systems Integration High-Level Design(s):** The Design and Integration Partner shall support the Authority with the integration of the DSA capability into existing and future training systems, where a DSA training requirement is identified. This shall include working collaboratively with any existing/future training system integrator in order to design, implement, integrate, test and roll-out suitable solutions for each training system.
20. **Support to the Authority/Authority’s third party supplier(s) Training Activity:** The Design and Integration Partner shall provide documentation/information (as requested by the Authority) to support the Authority/Authority’s third party suppliers in their training activities (which may include but shall not be limited to the undertaking of a Training Needs Analysis and/or the development of Training Design Documentation and/or the development of the Training Solution). The Design and Integration Partner shall review and comment on the Authority/Authority’s third-party supplier produced Training Documentation (as and when requested to do so by the Authority).
21. The above processes and ways of working shall be subject to amendment as the collaborative relationship between the Authority and the Design and Integration Partner develops, and improvements to the processes, procedures and way of working are identified, agreed and adapted by both parties during delivery of the contract.

CONTRACT OPTIONS

1. The Authority shall have the right to exercise the following contract option at its discretion:
2. **Option 1: 6-month continuation and handover of Design & Integration Partner Services.** The Design and Integration Partner shall continue to deliver the services detailed within this Statement of Requirement for a period of 6 months. The Design and Integration Partner shall conduct the necessary exit activities to transition the services to the BATCIS CDO and/or an incoming third-party supplier (to be advised by the Authority).

Annex A - Consolidated view of the Meetings, Deliverables and Supporting Activities associated with the Authority's Statement of Requirement

This Annex provides a consolidated view of the meetings, deliverables, supporting activities and the Authority's indicative timeframes associated with this Statement of Requirement document. The Design and Integration Partner shall work collaboratively with the Authority to produce realistic and achievable timelines for the deliverables, meetings and activities detailed within this Annex. This Annex shall be updated at Contract Award with the deliverable timeframes agreed between both parties.

**Meetings, Deliverables and Supporting Activities**

|  |  |  |  |
| --- | --- | --- | --- |
| Business Requirement | Description | Required By Date | Acceptance Criteria |
| 001 - Project & Programme Management | Onboarding: Provide personnel information (numbers, roles and experience, Security Clearance details) and sign any Non-Disclosure Agreements issued by the Authority. | At Contract Award | Agreement and acceptance by both parties. |
| Project kick-off meeting | Within 2 weeks of Contract Award | Attendance and contribution required. |
| Joint Relationship Management Plan (collaboratively developed) | Within 1 month of Contract Award | Agreement and acceptance by both parties. |
| Multilateral joint relationship meetings | As required | Attendance and contribution required |
| Weekly Project Meeting  Monthly Project Review  Quarterly Project Board | Weekly  Monthly  Quarterly | Attendance and contribution required. |
| Import and Export Management Log | As required | Acceptance by both parties. |
| 002 - Requirements, Architecture, Design & Engineering | Updated DSA System Architecture, including:   * Technical Drivers * Constraints, dependencies, assumptions   DSA System Design, including:   * System use cases - to support specification and requirement traceability * Subsystem Requirements Documents (SSRDs)/Technical Product Specifications for radio and components * Interface Control Documents * Supporting technical drawings/diagrams * System constraint information * Design decisions * Draft Bill of Materials, for both software and hardware system components. This Bill of Materials shall be further developed collaboratively between the Authority, Design and Integration Partner and the Authority's third-party suppliers (where applicable) * ROM costs   Radio Subsystem Requirements Document (SSRD)/Technical Product Specification | For PDR and updated for each Design Review thereafter  For PDR and updated for each Design Review thereafter  For RSDR | Agreement and acceptance by both parties.  All documentation to be updated in line with any changes. |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Electromagnetic Integration Management:   * E3 equipment certification specifications. * Technical drawings and/or models. * E3 Test Plans. * Test Readiness Review Output Documents. * E3 Test Reports. | As agreed between both parties | Agreement and acceptance by both parties. |
| HFI Reports | As agreed between both parties | Agreement and acceptance by both parties. |
| Formal Design Reviews:   * System Requirements Review (SRR) - expected to be within 3 months of Contract Award. * Radio Subsystem Design Review (RSDR) - expected to be within 6 months of Contract Award. * Preliminary Design Review (PDR) - expected to be within 6 months of Contract Award. * Interim Design Reviews (IDR) - expected to be within 12 and 18 months of Contract Award. * System Design Review (SDR) - expected to be within 24 months of Contract Award.   Documentation for Design Reviews  Design Review Actions and Decisions  Continuous Assurance design reviews and meetings - as required. | 15 working days prior to Design Review  Within 5 working days of Design Review | Attendance and contribution required.  Agreement and acceptance by both parties.  Agreement and acceptance by both parties.  Agreement and acceptance by both parties. |
| Review and maintenance of the Technical Library. | Monthly | Agreement and acceptance by both parties. |
| Technology Horizon Management Roadmap  This shall be updated as a minimum on a 6-monthly frequency or upon identification of a new technology (whichever is sooner) | Within 6 Months of Contract Award | Agreement and acceptance by both parties. |
| Obsolescence Management Plan  This shall be updated as a minimum on a 6-monthly frequency or upon identification an obsolescence issue (whichever is sooner)  Obsolescence Management Roadmap  This shall be updated as a minimum on a 6-monthly frequency or upon identification an obsolescence issue (whichever is sooner) | Within 6 months of Contract Award  Within 6 months of Contract Award | Agreement and acceptance by both parties. |
| Engineering Management Plan | Within 2 months of Contract Award | Agreement and acceptance by both parties. |
| Attendance at Authority Working Groups, including but not limited to design, training, integrated logistics support, security, safety, requirements, capability integration working groups | As required by the Authority | Attendance and contribution required. |
| 003 - Support to Authority Competitions | Statements of Work  Activities associated with the radio competition process, including but not limited to:   * Attendance at competition preparation meetings, Authority funded training sessions, competition process meetings, workshops * Conduct Lab Testing * Attendance at radio down-select trials | As required by the Authority | Agreement and acceptance by both parties.  Attendance and contribution as required. |

|  |  |  |  |
| --- | --- | --- | --- |
| 004 - Manage Change Control & Configuration Management | Change Request Form  Impact Information  Change Control Board  Change Impact Information  Joint Implementation Plan | As appropriate. | Agreement and acceptance by both parties.  Attendance and contribution as required. |
| Baseline Reference Set/Centre  Baseline Reference Management Plan  Baseline Reference Material Repository  Baseline Configuration Model | Within 6 months of Contract Award | Agreement and acceptance by both parties. |
| 005 - Manage System Integration | Developmental DSA System  Final Developmental DSA System | PDR & updated for each Design Review  For SDR | Agreement and acceptance by both parties. |
| Conformance Testing  DSA Design Conformance Test Schedule | As required by the Authority | Attendance and contribution required. |
| System Integration Test Report | For SDR | Agreement and acceptance by both parties. |
| 006 - System Design Authority, System Safety & System Security | DSA Safety and Environmental Management Plan (S&EMP) | At Contract Award |  |
| Part 2 (Design) Safety Case Report and supporting hazard log, analysis and evidence | Within 12 months of Contract Award | Agreement and acceptance by both parties. |
| DSA Safety and Environmental Management System (SEMS) | At Contract Award | Agreement and acceptance by both parties. |
| Safety Meetings  Safety Audits | As agreed between both parties | Attendance and contribution required. |
| Appointed Security POC | At Contract Award | Agreement and acceptance by both parties. |
| Design and Integration Partner Security Management Plan (SMP) | Within 1 month of Contract Award | Agreement and acceptance by both parties. |
| Security Assurance Case Reports  Security Impact Assessments  Security Cases  Design and Integration Partner Meeting Requests and Minutes/ROADs  DSA Security Operating Procedures (minimum of user and privileged user)  Design and Integration Partner Security Input to Test Plans | As agreed between both parties | Agreement and acceptance by both parties. |
| Design and Integration Partner owned Infrastructure Accreditation Artefacts and Management.  Supply Chain Security and Assurance Compliance Artefacts. | As agreed between both parties | Agreement and acceptance by both parties. |
| Accreditation, Security Assurance and Risk Management artefacts  A list of the above shall be provided by the Authority at Contract Award | As agreed between both parties | Agreement and acceptance by both parties. |
| Security Assurance Meetings | As required by the Authority | Attendance and contribution required. |
| Security Working Group: Quarterly.  DSA Security Meeting: Bi-Monthly.  DSA Security Risk Reviews: Monthly. | Quarterly  Bi-Monthly  Monthly | Attendance and contribution required. |
| DSA Public Key Infrastructure System Design  DSA PKI System Design Specifications  DSA Standalone PKI (for Developmental DSA System)  DSA PKI configuration data and test logs  Support user acceptance activities  DSA PKI Audit Database, event logs & SLA evidence | For PDR & updated for each Design Review  As required by the Authority | Agreement and acceptance by both parties. |
| 007 - Additional Ad-Hoc Tasking | As per tasking form | As per tasking form | As per tasking form. |
| 008 - Support to Training, Introduction to Service & Logistics Support | Development & Support Tools  Documentation on use and appropriate Training Material | For PDR and updated for each Design Review thereafter | Agreement and acceptance by both parties. |
| Software Support Plan, which shall include:   * Test Plans: Acceptance, System Integration, Regression, P&C. * System Integration Readiness Review Minutes. * Acceptance Test Readiness Review Minutes. * Acceptance Test Scripts. * Acceptance Test Reports. * Regression Test Report. * Regression Test Scripts. * System Integration Test Scripts. * System Integration Report. * Release Certificate. | Within 12 months of Contract Award | Agreement and acceptance by both parties. |
| Perpetual Licence Agreement for Any Proprietary Software developed during the Contract | As required by the Authority | Agreement and acceptance by both parties. |
| Technical Information for Technical Publications | As required by the Authority | Agreement and acceptance by both parties. |
| Integrated Support Plan | Within 12 months of Contract Award | Agreement and acceptance by both parties. |
| Documentation/information (as requested by the Authority) to support the Authority/Authority’s third-party suppliers in their training activities. | As required by the Authority | Agreement and acceptance by both parties. |

**Design and Integration Partner Support to Authority Led Activities**

|  |  |
| --- | --- |
| Business Requirement | Description |
| 001 - Project & Programme Management | Support the Authority with its reporting and governance activities. |
| Support the Authority in developing and maintaining the DSA RAIDO register, contribute to active risk management of the project, and provide status updates at the project meetings. |
| Provide support to the development of the DSA Collaborative Master Schedule and provide progress updates into the DSA Collaborative Master Schedule. |
| Provide support to any quality audit conducted by the Authority and/or Defence Digital Quality Assurance representatives and identify and implement any corrective actions raised at the earliest opportunity. |
| Share knowledge and best practise and support the Authority with identification and implementation of process improvements. |
| Provide support to the Authority in its assurance, approvals and Assessment Phase activities, including but not limited to development of Reports, Business Cases, Review Notes, Assurance and Approvals documentation, COEIAs. |
| 002 - Requirements, Architecture, Design & Engineering | Support the Authority through the Requirements and Acceptance end-to-end process. Support the Authority in concluding the requirements definition activities. |
| Support the Authority with development of the Systems Requirement Document for baseline at the System Requirements Review. |
| Support the Authority with the creation of a shared Technical Library, support the Authority in the identification, sourcing and maintenance of the necessary standards, policy, principles and guidelines required for the delivery of the contract. |
| Support the Authority in the development of a design repository structure (within the Technical Library) to hold all design and system integration documentation and software. Support the Authority in the implementation and management of the design repository, including: (1) File storage and information exchange process for the Authority, the Design and Integration Partner, and third-party supplier artefacts and software. (2) Document configuration change and action management tooling, to include the following capabilities: (a) Perform fully traceable document reviews and approval cycles. (b) Create actions in association to documents. (c) Document configuration changes with folder-based security access. (d) Formal repository, records and inventory database. (e) Customisable document metadata in accordance with the needs of a project or mission. (f) Ability to automate the creation of document reference numbers according to specific project or Authority departmental rules. (g) Dynamic search and export capability. (h) Multiple Author response tracking. (i) Audits. (j) Report generation. (k) Inability to remove files or folders to ensure that historical documentation is retained. |
| 003 - Support to Authority Competitions | Support the Authority in its competition activity for the Radio Provider and down-select trials. Support to preparation for the competition, support to the evaluation process and support to the radio down-select trials. Support the Authority with the production of documentation and technical work packages associated with the radio procurement:  Input to Contract Notice, DPQQ and DPQQ evaluation strategy, support Authority responses to clarification questions, conduct DPQQ evaluation, attend moderation of DPQQ evaluation, support to Authority preparation of debrief letters. Support to development of Statement of Requirement, support to production of supporting documentation, support to production of Evaluation Strategy, support to production of Negotiation Strategy (as applicable), support to production of Contract Terms and Conditions, support Authority responses to clarification questions, conduct Tender Evaluations, attend moderation of Tender Evaluations, support down select radio demonstrations and trials, support the Authority with preparation for negotiations, support negotiations, conduct Best And Final Offer (BAFO) evaluations, attend moderation of BAFO evaluations, support to Authority preparation of debrief letters. |
| 004 - Manage Change Control & Configuration Management | Support the Authority in the production of a Configuration Management Plan, applicable to both project and technical configuration management, feeding in best practise and ways of working. |
| 005 - Manage System Integration | Support the Authority in conducting evaluation and acceptance activities as part of the design review process. |
| Support the Authority with the management of verification and validation activities and provide the required evidence (as required). |
| Support the Authority's assurance activities on the Developmental DSA System. |
| 006 - System Design Authority (SDA), System Safety & System Security | Work collaboratively with the Authority on the production of Accreditation, Security Assurance and Risk Management artefacts that support the Accreditation and delivery of a secure and compliant DSA system. Input factual information and Design Collateral to help build the Accreditation Case. Support the Authority (as a key stakeholder) in designing a secure DSA and providing Assurance Evidence to the Authority. |
| Provide support to the Authority in the development of the following products and/or provide the Authority with the support to completion of the following activities: (a) DSA Technical Risk Assessment. (b) DSA/BATCIS Coordinating Design Organisation Security Risk Register. (c) DSA Project Crypto Plan. (d) DSA Risk Management and Accreditation Document Sets. (e) DSA Baseline Control Set. (f) DSA Accreditation Scoping Appraisal. (g) DSA Risk Treatment Plan. (h) National Cyber Security Centre Cloud Security Compliance Statement. (i) Information Security Management Plan. (j) DSA Security Working Group ROADs. (k) DSA Anti-Virus Policy. (l) DSA Digital Forensics Policy. (m) DSA Protective Monitoring Policy. (n) DSA Incident Management Policy. (o) DSA Patching Policy. (p) Information Technology Health Checks Scoping Documents. (q) ITHC Remediation Plans. (r) ITHC Remediation Tracker. (s) Vulnerability Assessments. (t) DSA Security Impact Assessments. (u) DSA Business Continuity Plan. (v) DSA Data Management Plan. (w) DSA Authority to Test Management Plan. (x) DSA Risk Balanced Cases. (y) DSA Security Grading Guide. (z) Security Assurance Case Report. (aa) SWG Minutes. |
| 008 - Support to Training, Introduction to Service & Logistics Support | Provide support (as requested by the Authority) to the Authority to produce the required DSA Technical Publications. Review and comment on the Authority produced Technical Publications (as and when requested to do so by the Authority). |
| Support the Authority with the integration of the DSA capability into existing and future training systems, where a DSA training requirement is identified. Work collaboratively with any existing/future training system integrator in order to design, implement, integrate, test and roll-out suitable solutions for each training system. |
| Review and comment on the Authority/Authority’s third-party supplier produced Training Documentation (as and when requested to do so by the Authority). |

**Option 1 - Delivery of the services detailed within this Statement of Requirement for an additional 6-month period**

|  |  |  |  |
| --- | --- | --- | --- |
| Business Requirement | Description | Required By Date | Acceptance Criteria |
| All | Delivery of the services detailed within this Statement of Requirement for an additional 6-month period. Conduct exit activities to transition the service to the Authority's CDO or an incoming supplier. | 6 months from contract option being invoked | Agreement and acceptance by both parties. |

Annex B - Record of Government Furnished Assets issued to the Design and Integration Partner

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **GFE Item** | **Type of GFA** | **Qty** | **Terms of Loan** | **Date of Supply** | **Date of return** | **Reporting** | **Maintenance responsibility** | **Responsibility for delivery** | **Disposal/return arrangements** |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

**Worker Engagement Route (including IR35 status):** This requirement of outside of IR35

## Call-Off Schedule 26 (Cyber Essentials Scheme)

### Definitions

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

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Cyber Essentials Scheme** | 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 are at: <https://www.cyberessentials.ncsc.gov.uk/>; |
| **Cyber Essentials Basic Certificate** | 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** | Cyber Essentials Basic Certificate or the Cyber Essentials Plus Certificate to be provided by the Supplier as set out in the Order Form; |
| **Cyber Essential Scheme Data** | sensitive and personal information and other relevant information as referred to in the Cyber Essentials Scheme; and |
| **Cyber Essentials Plus Certificate** | 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. |

### What Certification do you need

* 1. Where the Order Form requires that the Supplier provide a Cyber Essentials Certificate or Cyber Essentials Plus Certificate prior to commencing the provision of Deliverables the Supplier shall provide a valid Cyber Essentials Certificate or Cyber Essentials Plus Certificate to the Buyer. Where the Supplier fails to comply with this Paragraph it shall be prohibited from commencing the provision of Deliverables under the Call-Off Contract until such time as the Supplier has evidenced to the Buyer its compliance with this Paragraph 2.1.
  2. Where the Supplier continues to process data during the Call-Off Contract Period the Supplier shall deliver to the Buyer evidence of renewal of the Cyber Essentials Certificate or Cyber Essentials Plus Certificate on each anniversary of the first applicable certificate obtained by the Supplier under Paragraph 2.1.
  3. In the event that the Supplier fails to comply with Paragraph 2.1 or 2.2, the Buyer reserves the right to terminate the Call-Off Contract for material Default.
  4. The Supplier shall ensure that all Sub-Contracts with Subcontractors who Process Cyber Essentials Data contain provisions no less onerous on the Subcontractors than those imposed on the Supplier under the Call-Off Contract in respect of the Cyber Essentials Scheme under Paragraph 2.1 of this Schedule.
  5. This Schedule shall survive termination of each and any Call-Off Contract.

1. <https://www.aof.mod.uk> [↑](#footnote-ref-2)
2. <https://www.aof.mod.uk/aofcontent/tactical/software/content/sw_requirements.htm> [↑](#footnote-ref-3)
3. <https://www.aof.mod.uk/aofcontent/tactical/software/content/sw_support_requirements.htm> [↑](#footnote-ref-4)
4. <https://www.aof.mod.uk/aofcontent/tactical/software/content/sw_documentation.htm> [↑](#footnote-ref-5)
5. A light role infantry company has a minimum of 28 commanders, ranging from Lance-Corporal to Major, who are responsible for 120 to 150 soldiers. [↑](#footnote-ref-6)
6. Of the Concept, Assessment, Demonstration, Manufacture, In Service, Disposal (CADMID) cycle. [↑](#footnote-ref-7)
7. Being constrained or tied into a vendor/set of vendors' products or services due to proprietary issues or substantial switching costs associated with changing vendors. [↑](#footnote-ref-8)
8. This detail is being provided as information only to set the context. The Radio Provider and component provider are separate contracts to the Design and Integration Partner; and outside the scope of this Statement of Requirement. [↑](#footnote-ref-9)
9. Meaning on foot not in vehicles. [↑](#footnote-ref-10)
10. The proposed DSA capability shall store, display and transmit data and information up to Official Sensitive only. [↑](#footnote-ref-11)
11. Mounted close combat refers to the capability that utilises vehicles when ‘closing with and destroying the enemy’ and includes main battle tanks, armoured fighting vehicles and protected mobility vehicles. The requirement for mounted close combat is outside the scope of this Statement of Requirement document. [↑](#footnote-ref-12)
12. The Authority will be the ultimate decision maker at the design board. [↑](#footnote-ref-13)
13. There is a need for a small number of Design and Integration Partner personnel to access Secret UK Eyes Only (SUKEO) reference material. Security Check (SC) vetting shall be required for those personnel the Design and Integration Partner considers need access to Authority SUKEO reference material. As part of the onboarding process, the Design and Integration Partner shall provide details of a minimum of 2 x personnel with SC clearance to access SUKEO reference material. [↑](#footnote-ref-14)
14. Projects in Controlled Environments. [↑](#footnote-ref-15)
15. To be agreed between the Design and Integration Partner and the Authority upon Contract Award. [↑](#footnote-ref-16)
16. All requirements documents shall be managed by the Authority in the Authority’s Dynamic Object-Oriented Requirements System (DOORS) requirements management tool. [↑](#footnote-ref-17)
17. Based on the work already completed by the Authority. [↑](#footnote-ref-18)
18. The DSA System Architecture shall fully specify the design down to the component level. [↑](#footnote-ref-19)
19. Further details of the MOD Design Review process can be found on the KiD Portal. [↑](#footnote-ref-20)
20. The Design and Integration Partner shall ensure all personnel assigned to the project have a working knowledge and understanding of the necessary standards, policy, principles and guidelines published by the MOD. [↑](#footnote-ref-21)
21. A Commerce Decisions tool used by the Authority in competitive procurements; helps buyers to confidently and efficiently select the best supplier. [↑](#footnote-ref-22)
22. In a format to be agreed between both parties. [↑](#footnote-ref-23)
23. Assumed standalone (see DSA Background Technical Information document for design assumptions). [↑](#footnote-ref-24)