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

**Order Form**

CALL-OFF REFERENCE: **CCTS24A20**

THE BUYER: **Cabinet Office**

BUYER ADDRESS **70 Whitehall**

**LONDON**

**SW1A 2AS**

**England**

THE SUPPLIER: **Covoxa Limited**

SUPPLIER ADDRESS: **45 Stockbridge Road, Winchester, SO22 6RW**

REGISTRATION NUMBER: **07359811**

DUNS NUMBER: **TBC at Contract Award**

SID4GOV ID: **TBC at Contract Award**

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated **22 January 2025**

It’s issued under the Framework Contract with the reference number RM6193 for the provision of Software Design and Implementation Services.

CALL-OFF INCORPORATED TERMS

The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM6193
3. The following Schedules in equal order of precedence:

* Joint Schedules for **RM6193**
  + Joint Schedule 2 (Variation Form)
  + Joint Schedule 3 (Insurance Requirements)
  + Joint Schedule 4 (Commercially Sensitive Information)
  + Joint Schedule 6 (Key Subcontractors)
  + Joint Schedule 7 (Financial Difficulties)
  + Joint Schedule 8 (Guarantee)
  + Joint Schedule 9 (Minimum Standards of Reliability)
  + Joint Schedule 10 (Rectification Plan)
  + Joint Schedule 11 (Processing Data)
  + Joint Schedule 12 (Supply Chain Visibility)
* Call-Off Schedules for **CCTS24A20**
  + Call-Off Schedule 1 (Transparency Reports)
  + Call-Off Schedule 3 (Continuous Improvement)
  + Call-Off Schedule 5 (Pricing Details)
  + Call-Off Schedule 6 (ICT Services)
  + Call-Off Schedule 7 (Key Supplier Staff)
  + Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
  + Call-Off Schedule 9 (Security)
  + Call-Off Schedule 10 (Exit Management)
  + Call-Off Schedule 11 (Installation Works)
  + Call-Off Schedule 13 (Implementation Plan and Testing)
  + Call-Off Schedule 14 (Service Levels)
  + Call-Off Schedule 15 (Call-Off Contract Management)
  + Call-Off Schedule 16 (Benchmarking)
  + Call-Off Schedule 18 (Background Checks)
  + Call-Off Schedule 20 (Call-Off Specification)

1. Special Schedule 1 (Statement of Works Mechanism and Template)
2. CCS Core Terms (version 3.0.10)
3. Call-Off Schedule 4 (Call-Off Tender)
4. Joint Schedule 5 (Corporate Social Responsibility) RM6193

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

**CALL-OFF SPECIAL TERMS**

The following Special Terms are incorporated into this Call-Off Contract. Drafting highlighted in red is new or amended drafting. For ease of reference, this Order Form incorporates new terms into the Call-Off. Contract documents as follows:

**Schedules amended by the Special Terms set out in pages 3-6 (inclusive) of this Order Form:**

1. CCS Core Terms (Version 3.0.10)
2. Joint Schedule 1 (Definitions and Interpretation)
3. Joint Schedule 2 (Variation Form)
4. Joint Schedule 7 (Financial Difficulties)
5. Joint Schedule 11 (Processing Data)
6. Call-Off Schedule 1 (Transparency Reports)
7. Call-Off Schedule 2 (Staff Transfer)
8. Call-Off Schedule 6 (ICT Services)
9. Call-Off Schedule 10 (Exit Management)
10. Call-Off Schedule 13 (Implementation Plan and Testing)
11. Call-Off Schedule 15 (Call-Off Contract Management)

**Schedules replaced entirely or added as new Special Schedules and appended to this Order Form:**

1. Special Schedule 1 (Statement of Work Mechanism and Template) - Appendix 1
2. Call-Off Schedule 5 (Pricing Details) - Appendix 4
3. Call-Off Schedule 9 (Security) - Appendix 2
4. Call-Off Schedule 14 (Service Levels) - Appendix 3
5. Call-Off Schedule 20 (Specification) - Appendix 5

**Special Terms relating to statements of work:**

|  |  |
| --- | --- |
| Definition of “Key Personnel” in Joint Schedule 1 (Definition and Interpretation) amended: | This definition is amended to read as follows:  “Key Personnel” the individuals (if any) identified as such in the Order  Form and/or in any Statement of Work.” |
| Definition of “Implementation Plan” in Joint Schedule 1 (Definitions and Interpretation) amended: | This definition is amended to read as follows:  “Implementation Plan” plan for provision of the Deliverables set out in  Call-Off Schedule 13 (Implementation Plan and Testing) where that  Schedule is used or otherwise as agreed between the Supplier and the  Buyer as may be supplemented by any Statement of Work subsequently  agreed by the Parties;” |
| Definition of “SOW Start Date” in Joint Schedule 1 (Definitions and Interpretation) amended: | This definition is amended to read as follows:  “SOW Start Date” the date of start of the relevant Statement of Work  as stated in the Statement of Work Details section of such Statement of  Work.” |
| Definition of “SOW End Date” in Joint Schedule 1 (Definitions and Interpretation) amended: | This definition is amended as follows:  ““SOW End Date” the date up to and including this date when the supply  of the Deliverables under the Statement of Work shall cease as stated in  the Statement of Work Details section of such Statement of Work.” |
| Definition of “Statement of Works” “(SOW)” in Joint Schedule 1 | This definition is amended to read as follows:  ““Statement of Work” “(SOW)” the document, set out and agreed in  accordance with Special Schedule 1 (Statement of Work Mechanism and  Template) which, upon its execution by the Buyer and Supplier, shall  become incorporated into their Call-Off Contract and outlines the agreed  body of works to be undertaken as part of the Call-Off Contract  Deliverables. There may be any number of Statements of Work  incorporated into a Call-Off Contract and each Statement of Work may  include (but is not limited to) the Statement of Requirements, identified  output(s), completion date(s) and charging method(s);” |
| Opening paragraph in Joint Schedule 2  (Variation Form) amended: | This paragraph is amended to read as follows:  “This form is to be used in order to change a Contract in accordance with Clause 24 (Changing the Contract) and shall in no way prejudice the  Statement of Work mechanism set out in set out in Special Schedule 1  (Statement of Work Mechanism and Template).” |
| Paragraph 3 in Joint Schedule 2 (Variation Form) amended: | “The Call-Off Contract, including any previous Variations and any  Statements of Work, shall remain effective and unaltered except as  amended by this Variation.” |
| Definition of “Statement of Work 1” added to Joint Schedule 1 (Definitions and Interpretation): | A new definition is inserted as follows:  ““Statement of Work 1” the first Statement of Work to be executed and  incorporated into this Call-Off Contract;” |
| Special Schedule 1 (Statement of Work  Mechanism and Template) added: | This schedule is inserted into the Call-Off Contract in the form appended  to this Framework Schedule 6 (Order Form Template and Call-Off  Schedules) in Appendix 1. |
| Clause 24.9 in CCS Core Terms (version 3.0.10) for RM6193 added: | This clause is inserted as follows:  “24.9 Nothing in this clause 24 (Changing the Contract) shall prejudice  the Statement of Work mechanism. For the avoidance of doubt, the  request of any Statement of Work shall be implemented by the  mechanism set out in Special Schedule 1 (Statement of Work Mechanism  and Template) and not this clause 24 or any provisions related to the  Variation mechanism and Variation Form referred to in this Call-Off  Contract.” |

**Special Terms relating to security:**

|  |  |
| --- | --- |
| Call-Off Schedule 9 (Security) | Deleted in its entirety and replaced with Security Management Schedule (Consultancy) |

**Special Terms relating to Service Levels:**

|  |  |
| --- | --- |
| Definition of “Service Level” in Joint Schedule 1 (Definitions and Interpretation) amended: | This definition is amended to read as follows:  ““Service Levels” service levels applicable to the provision of the  Deliverables under the Call-Off Contract specified in the Annex to Part A  of Call Off Schedule 14 (Service Levels) (as reasonably amended or  updated by the Buyer from time to time) and/or in the Statement of Work  applicable to the relevant Services) and which for the avoidance of doubt  shall include any key performance indicator set out in such document;” |
| Definition of “Service Credits” in Call-Off Schedule 14 (Service Levels) amended: | This definition is amended to read as follows:  ““Service Credits” any service credits specified in the Annex to Part A of  this Schedule (as reasonably amended or updated by the Buyer from time  to time) being payable by the Supplier to the Buyer in respect of any  failure by the Supplier to meet one or more Service Levels;” |

**Special Terms relating to Pricing Details:**

|  |  |
| --- | --- |
| Call-Off Schedule 5 (Pricing Details) | This schedule is amended in the form appended to this Framework  Schedule 6 (Order Form Template and Call-Off Schedules) in Appendix  5. |

CALL-OFF START DATE: **24 January 2025**

CALL-OFF EXPIRY DATE: **23 January 2027**

CALL-OFF INITIAL PERIOD: **Two (2) Years**

CALL-OFF DELIVERABLES

See details in Call-Off Schedule 20 (Call-Off Specification)

MAXIMUM LIABILITY

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is£2,000,000.00 excluding VAT

CALL-OFF CHARGES

See details in Call-Off Schedule 5 (Pricing Details)]

All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4, 5 and 6 (if used) in Framework Schedule 3 (Framework Prices)

REIMBURSABLE EXPENSES

None

PAYMENT METHOD

Invoices should be raised on a monthly basis for progress made against each of the key programme deliverables (as agreed with the Project Manager and Head of PMO)

The Buyer will make payments via BACS

BUYER’S INVOICE ADDRESS:

**REDACTED TEXT under FOIA Section 40, Personal Information**

BUYER’S AUTHORISED REPRESENTATIVE

**REDACTED TEXT under FOIA Section 40, Personal Information**

BUYER’S ENVIRONMENTAL POLICY

Cabinet Office’s additional sustainability requirements are available online at: <https://www.gov.uk/government/publications/cabinet-office-environmental-policy-statement/cabinet-office-environmental-policy-statement>

BUYER’S SECURITY POLICY

Security Management Plan, please refer to Call-Off Schedule 9

SUPPLIER’S AUTHORISED REPRESENTATIVE

**REDACTED TEXT under FOIA Section 40, Personal Information**

SUPPLIER’S CONTRACT MANAGER

**REDACTED TEXT under FOIA Section 40, Personal Information**

PROGRESS REPORT FREQUENCY

Monthly - Highlight report update meetings (with the Programme Director and MyCO Senior leadership team)

PROGRESS MEETING FREQUENCY

Monthly - Progress review and payment authorisation meetings to follow highlight report meeting (with the Programme Manager, Finance and Resourcing Lead and Senior Leadership Team)

KEY STAFF

**REDACTED TEXT under FOIA Section 40, Personal Information**

KEY SUBCONTRACTOR(S)

**NONE**

COMMERCIALLY SENSITIVE INFORMATION

Supplier Tender and Pricing

SERVICE CREDITS

Please refer to Appendix 3 and Call-Off Schedule 14 (Service Levels)

ADDITIONAL INSURANCES

● a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract.

● professional indemnity insurance cover to be held by the Supplier and by any agent,

Subcontractor or consultant involved in the supply of Services. This professional

indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for

each individual claim or any higher limit the Buyer requires (and as required by Law).

● employers' liability insurance with a minimum limit of £5,000,000 or any higher

minimum limit required by Law.

GUARANTEE

There’s a guarantee of the Supplier’s performance provided for all Call-Off Contracts entered under the Framework Contract.

SOCIAL VALUE COMMITMENT

The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender)]

|  |  |  |  |
| --- | --- | --- | --- |
| For and on behalf of the Supplier: | | For and on behalf of the Buyer: | |
| Signature: | REDACTED TEXT under FOIA Section 40, Personal Information | Signature: | REDACTED TEXT under FOIA Section 40, Personal Information |
| Name: | REDACTED TEXT under FOIA Section 40, Personal Information | Name: | REDACTED TEXT under FOIA Section 40, Personal Information |
| Role: | REDACTED TEXT under FOIA Section 40, Personal Information | Role: | REDACTED TEXT under FOIA Section 40, Personal Information |
| Date: |  | Date: |  |

Appendix 1

# Special Schedule 1 (Statement of Work Mechanism and Template)

## Part 1: Statement of Work Mechanism

1. **Statements of Work**
   1. Both Parties acknowledge and agree that Statements of Work are required for performance of each Party’s obligations under this Call-Off Contract.
   2. The Buyer may procure any of the Services by agreeing a Statement of Work with the Supplier pursuant to this Special Schedule 1 (Statement of Work Mechanism and Template) and the Supplier shall provide such Services from the date specified in the relevant Statement of Work.
   3. During the Call-Off Contract Period, the Buyer and Supplier may agree and execute completed Statement(s) of Work. Upon execution of a Statement of Work the provisions detailed therein shall be incorporated into this Call-Off Contract.
   4. Each Statement of Work shall be part of this Call-Off Contract and shall not form a separate contract to it.
   5. Each Statement of Work shall fall within the provisions of the Call-Off Contract.
   6. For the avoidance of doubt, the Buyer has no obligation to award Statements of Work in relation to any of the workstreams that sit outside of the fixed price deliverables under this Call-Off Contract or at all. In making any decision in respect of awarding any Statement of Work in relation to Support and Maintenance Services, the Buyer shall be entitled at its discretion to take into consideration the outcome of any Benchmark Review or Benchmarking Report in respect of the Support and Maintenance Services.
2. **Agreeing and executing Statements of Work**
   1. The first Statement of Works shall be inserted into Annex 1 as part of the executed Order Form.
   2. Each Statement of Work that has been completed in the form of the Statement of Work Template set out in Part 2 of this Special Schedule 1 (Statement of Work Mechanism and Template) and agreed in accordance with paragraph 2.4 of this Part 1 of Special Schedule 1 (Statement of Work Mechanism and Template) shall be executed by the Buyer and Supplier.
   3. Each executed Statement of Work shall be inserted into Annex 1 of this Special Schedule 1 (Statement of Work Mechanism and Template) in chronology.
   4. Each Statement of Work shall be agreed in the following manner:
      1. (a) the Buyer shall ask the Supplier to prepare a draft Statement of Work for Services required by the Buyer in the form of the Statement of Work Template set out in Part 2 of this Special Schedule 1 (Statement of Work Mechanism and Template);
      2. (b) within 10 Working Days of the Buyer’s request, the Supplier shall notify the Buyer of any additional information it reasonably requires in order to prepare a Statement of Work;
      3. (c) within 10 Working Days of receipt of the required information from the Buyer, the Supplier shall provide the Buyer with the draft Statement of Work Requested;
      4. (d) the Supplier and the Buyer shall discuss and agree that draft Statement of Work; and
      5. (e) both parties shall execute the draft Statement of Work when it is agreed.
   5. Once a Statement of Work has been agreed and signed in accordance with paragraph 2.4 of this Part 1 of Special Schedule 1 (Statement of Work Mechanism and Template), no amendment shall be made to it except in accordance with clause 24 (Changing the Contract) of CCS Core Terms (version 3.0.10) for RM6193.
3. **Charges.** Unless otherwise agreed, the sums payable for the Services provided under a Statement of Work shall be calculated in accordance with the Charges.
4. **Disputes over Statement(s) of Work.** In the event that a Statement of Work cannot be agreed in accordance with paragraph 2.4 of this Part 1 of Special Schedule 1 (Statement of Work Mechanism and Template), the Parties shall follow the procedure for resolving Disputes set out in clause 34 (Resolving Disputes) of CCS Core Terms (version 3.0.10) for RM6193.

## Part 2: Statement of Work Template

The details set out within this Statement of Work apply only in relation to the

Deliverables detailed herein and will not apply to any other Statements of Work

executed or to be executed under this Call-Off Contract, unless otherwise agreed by

the Parties in writing.

By signing this Statement of Work, the Parties agree that it shall be incorporated

into Annex 1 of Appendix 1 of the Order Form and incorporated into the Call-Off

Contract and be legally binding on the Parties:

|  |  |
| --- | --- |
| 1. Statement of Work Details | |
| Call-Off Reference: |  |
| Buyer: |  |
| Supplier: |  |
| SOW Number: |  |
| SOW Start Date: |  |
| SOW End Date: |  |
| SOW Duration: |  |
| SOW Charge: |  |
| Key Personnel (Buyer): |  |
| Key Personnel (Supplier): |  |
| 1. Buyer Obligations | |
| Buyer Obligations: |  |
| 1. Deliverables | |
| General Overview: |  |
| Deliverables: |  |
| |  |  |  | | --- | --- | --- | | Deliverables Description | Acceptable Criteria | Due date | |  |  |  | |  |  |  | |  |  |  | | |
| 1. Performance Management | |
| Applicable Service Levels: |  |
| 1. Other |  |
| Additional Requirements: |  |

**Signed for an on behalf of the Buyer:**

|  |  |
| --- | --- |
| Signature |  |
| Name |  |
| Role |  |
| Date |  |

**Signed for an on behalf of the Supplier:**

|  |  |
| --- | --- |
| Signature |  |
| Name |  |
| Role |  |
| Date |  |

Appendix 2

Call-Off Schedule 9 (Security Management: (Consultancy/Professional Services)

# Buyer Options

**Risk assessment**

|  |  |  |
| --- | --- | --- |
| The Buyer has assessed this Agreement as | a standard consultancy agreement | ☐ |
| a higher-risk consultancy agreement | X |

**Relevant Certifications**

|  |  |  |
| --- | --- | --- |
| Where the Buyer has assessed this Agreement as a standard consultancy agreement, it requires the Supplier to be certified as compliant with: | Cyber Essentials | ☐ |
| Cyber Essentials Plus | X |

# Supplier obligations

## Where the Buyer has assessed this Agreement as a higher-risk consultancy agreement, the Supplier must comply with all requirements in this Schedule 2 (Security Management).

## Where the Buyer has assessed this Agreement as a standard consultancy agreement, the Supplier must comply with this Schedule [x] (Security Management), other than:

### the requirement to be certified as compliant with ISO/IEC 27001:2013 under Paragraph 7.1(b);

### the requirement to undertake security testing of the Supplier Information Management System in accordance with paragraph 3 of Appendix 1;

### the requirement to produce a Security Management Plan in accordance with Paragraph 8

### the requirement to document unencrypted Buyer Data in the Security Management Plan in accordance with paragraph 5.4 of Appendix 1

# Definitions

* 1. In this Schedule 2 (Security Management):

|  |  |
| --- | --- |
| * 1. “Anti-virus Software” | means software that:  protects the Supplier Information Management System from the possible introduction of Malicious Software;   * + 1. scans for and identifies possible Malicious Software in the Supplier Information Management System;     2. if Malicious Software is detected in the Supplier Information Management System, so far as possible:        1. prevents the harmful effects of the Malicious Software; and        2. removes the Malicious Software from the Supplier Information Management System. |
| * 1. “Breach of Security” | * 1. means the occurrence of:      1. any unauthorised access to or use of the Services, the Buyer Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement;      2. the loss (physical or otherwise) and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement; and/or      3. any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements. |
| * 1. “Buyer Data” | * 1. means any:      1. data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media; or      2. Personal Data for which the Buyer is a, or the, Data Controller,   2. that is:      + 1. supplied to the Supplier by or on behalf of the Buyer; or        2. that the Supplier generates, processes, stores or transmits under this Agreement. |
| * 1. “Buyer Equipment” | * 1. means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System. |
| * 1. “Buyer System” | * 1. means the information and communications technology system used by the Buyer to interface with the Supplier Information Management System or through which the Buyer receives the Services. |
| * 1. “Certification Default” | * 1. means the occurrence of one or more of the circumstances listed in paragraph 7.4. |
| * 1. “Certification Rectification Plan” | * 1. means the plan referred to in paragraph 7.5(a). |
| * 1. “Certification Requirements” | * 1. means the information security requirements set out in paragraph 7. |
| * 1. “Cyber Essentials” | * 1. means the Cyber Essentials certificate issued under the Cyber Essentials Scheme. |
| * 1. “Cyber Essentials Plus” | * 1. means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme. |
| * 1. “Cyber Essentials Scheme” | * 1. means the Cyber Essentials scheme operated by the National Cyber Security Centre. |
| * 1. “End-user Device” | * 1. means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services. |
| * 1. “HMG Baseline Personnel Security Standard” | * 1. means the employment controls applied to any individual member of the Supplier Personnel that performs any activity relating to the provision or management of the Services, as set out in “HMG Baseline Personnel Standard”, Version 6.0, May 2018 https://assets.publishing.service.gov.uk /government/uploads/system/uploads/attachment\_data/file/714002/HMG\_Baseline\_Personnel\_Security\_Standard\_-\_May\_2018.pdf), as that document is updated from time to time. |
| * 1. “Malicious Software” | * 1. means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations. |
| * 1. “NCSC Cloud Security Principles” | * 1. means the National Cyber Security Centre’s document “Implementing the Cloud Security Principles” as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles. |
| * 1. “NCSC Device Guidance” | * 1. means the National Cyber Security Centre’s document “Device Security Guidance”, as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance. |
| * 1. “Privileged User” | * 1. means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges. |
| * 1. “Process” | * 1. means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data. |
| * 1. “Prohibited Activity” | * 1. means the storage, access or Processing of Buyer Data prohibited by a Prohibition Notice. |
| * 1. “Prohibition Notice” | * 1. means a notice issued under paragraph 1.3 of Appendix 1. |
| * 1. “Relevant Certifications” | * 1. means those certifications specified in paragraph 7.1. |
| * 1. “Relevant Convictions” | * 1. means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), or any other offences relevant to Services as the Buyer may specify. |
| * 1. “Security Management Plan” | * 1. means the document prepared in accordance with the requirements of paragraph 8. |
| * 1. “Sites” | * 1. means any premises:      1. from or at which:         1. the Services are (or are to be) provided; or         2. the Supplier manages, organises or otherwise directs the provision or the use of the Services; or      2. where:         1. any part of the Supplier Information Management System is situated; or         2. any physical interface with the Buyer System takes place. |
| * 1. “Standard Contractual Clauses” | * 1. means the standard data protection clauses specified in Article 46 of the United Kingdom General Data Protection Regulation setting out the appropriate safeguards for the transmission of personal data outside the combined territories of the United Kingdom and the European Economic Area. |
| * 1. “Supplier Information Management System” | * 1. means:      1. those parts of the information and communications technology system and the Sites that the Supplier or its Sub-contractors will use to provide the Services; and      2. the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources); |
| * 1. “Sub-contractor Personnel” | * 1. means:      1. any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and      2. engaged in or likely to be engaged in:         1. the performance or management of the Services;         2. or the provision of facilities or services that are necessary for the provision of the Services. |
| * 1. “Supplier Personnel” | * 1. means any individual engaged, directly or indirectly, or employed by the Supplier or any Sub-contractor in the management or performance of the Supplier’s obligations under this Agreement. |
| * 1. “UKAS” | * 1. means the United Kingdom Accreditation Service. |

# Introduction

## This Schedule 2 (Security Management) sets out:

### the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Agreement to ensure the security of the Buyer Data, the Services and the Supplier Information Management System;

### the assessment of this Agreement as either a:

#### standard consultancy agreement; or

#### higher-risk consultancy agreement,

in paragraph 1;

### the Buyer’s access to the Supplier Personnel and Supplier Information Management System, in paragraph 6;

### the Certification Requirements, in paragraph 7;

### the requirements for a Security Management Plan in the case of higher-risk consultancy agreements, in paragraph 8; and

### the security requirements with which the Supplier and Sub-contractors must comply in Appendix 1.

# Principles of security

## The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Buyer Data and, consequently on the security of:

### the Sites;

### the Services; and

### the Supplier’s Information Management System.

## The Supplier is responsible for:

### the security, confidentiality, integrity and availability of the Buyer Data when that Buyer Data is under the control of the Supplier or any of its Sub-contractors; and

### the security of the Supplier Information Management System.

## The Supplier:

### comply with the security requirements in Appendix 1; and

### ensure that each Sub-contractor that Processes Buyer Data complies with the security requirements in Appendix 1.

## Where the Supplier, a Sub-contractor or any of the Supplier Personnel is granted access to the Buyer System or to the Buyer Equipment, it must comply with and ensure that all such Sub-contractors and Supplier Personnel comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Buyer System or the Buyer Equipment.

# Access to Supplier Personnel and Supplier Information Management System

## The Buyer may require, and the Supplier must provide the Buyer and its authorised representatives with:

### access to the Supplier Personnel;

### access to the Supplier Information Management System to audit the Supplier and its Sub-contractors’ compliance with this Agreement; and

### such other information and/or documentation that the Buyer or its authorised representatives may reasonably require,

* 1. to assist the Buyer to establish whether the arrangements which the Supplier and its Sub-contractors have implemented in order to ensure the security of the Buyer Data and the Supplier Information Management System are consistent with the representations in the Security Management Plan.

## The Supplier must provide the access required by the Buyer in accordance with paragraph 6.1 within ten Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Buyer with the access that it requires within 24 hours of receipt of such request.

# Certification Requirements

## The Supplier shall ensure that, unless otherwise agreed by the Buyer, it is certified as compliant with:

### in the case of a standard consultancy agreement the option chosen by the Buyer in Paragraph 1; or

### in the case of a higher-risk consultancy agreement:

#### ISO/IEC 27001:2013 by a UKAS-approved certification body in respect of the Supplier Information Management System, or the Supplier Information Management System is included within the scope of a wider certification of compliance with ISO/IEC 27001:2018; and

#### Cyber Essentials Plus (“Relevant Certifications”).

## Unless otherwise agreed by the Buyer, the Supplier must provide the Buyer with a copy of the Relevant Certifications before it begins to provide the Services.

## The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications are:

### currently in effect;

### relate to the full scope of the Supplier Information System; and

### are not subject to any condition that may impact the provision of the Services.

## The Supplier must notify the Buyer promptly, any in any event within three Working Days of becoming aware that:

### a Relevant Certification has been revoked or cancelled by the body that awarded it;

### a Relevant Certification expired and has not been renewed by the Supplier;

### a Relevant Certification no longer applies to the full scope of the Supplier Information Management System or

### the body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a “Certification Default”).

## Where the Supplier has notified the Buyer of a Certification Default under paragraph 7.4:

### the Supplier must, within ten working Days of the date in which the Supplier provided notice under paragraph 7.4 (or such other period as the Parties may agree) provide a draft plan (a “Certification Rectification Plan”) to the Supplier setting out:

#### full details of the Certification Default, including a root cause analysis;

#### the actual and anticipated effects of the Certification Default;

#### the steps the Supplier will take to remedy the Certification Default;

### the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;

### if the Buyer rejects the Certification Rectification Plan, the Buyer must within five Working Days of the date of the rejection submit a revised Certification Rectification Plan and paragraph 7.5(b) will apply to the re-submitted plan;

### the rejection by the Buyer of a revised Certification Rectification Plan is a material Default of this Agreement;

### if the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

# Security Management Plan

## This paragraph 8 applies only where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.

**Preparation of Security Management Plan**

## The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Schedule 2 (Security Management) and the Agreement in order to ensure the security of the Buyer Data and the Supplier Information Management System.

## The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Call-Off Contract, the Security Management Plan, which must include:

### an assessment of the Supplier Information Management System against the requirements of this Schedule 2 (Security Management), including Appendix 1

### the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Buyer Data, the Buyer, the Services and/or users of the Services; and

### the following information in respect of each Sub-contractor:

#### the Sub-contractor’s:

##### legal name;

##### trading name (if any);

##### registration details (where the Sub-contractor is not an individual);

#### the Sites used by the Sub-contractor;

#### the Buyer Data Processed by the Sub-contractor;

#### the Processing that the Sub-contractor will undertake in respect of the Buyer Data;

#### the measures the Sub-contractor has in place to comply with the requirements of this Schedule 2 (Security Management).

## The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and must issue the Supplier with either:

### an information security approval statement, which shall confirm that the Supplier may use the Supplier Information Management System to Process Buyer Data; or

### a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.

## If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within ten Working Days of the date of the rejection, or such other period agreed with the Buyer.

**Updating Security Management Plan**

## The Supplier shall regularly review and update the Security Management Plan, and provide such to the Buyer, at least once each year and as required by this paragraph.

**Monitoring**

## The Supplier shall notify the Buyer within two Working Days after becoming aware of:

### a significant change to the components or architecture of the Supplier Information Management System;

### a new risk to the components or architecture of the Supplier Information Management System;

### a vulnerability to the components or architecture of the Supplier Information Management System using an industry standard vulnerability scoring mechanism;

* + 1. a change in the threat profile;

### a significant change to any risk component;

### a significant change in the quantity of Personal Data held within the Service;

### a proposal to change any of the Sites from which any part of the Services are provided; and/or

### an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

## Within ten Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Security Management Plan and submit the updated Security Management Plan to the Buyer for review and approval.

Appendix 1: Security requirements

1. **Location**
   1. Unless otherwise agreed with the Buyer, the Supplier must, and must ensure that its Sub-contractors must, at all times, store, access or process Buyer Data either:
      1. in the United Kingdom;
      2. the European Economic Area; or
      3. in a facility operated by an entity where:
         1. the entity has entered into a binding agreement with the Supplier or Sub-contractor (as applicable);

#### that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Sub-contractors in this Schedule 2 (Security Management);

* + - 1. the Supplier or Sub-contractor has taken reasonable steps to assure itself that
         1. the entity complies with the binding agreement;
         2. any system operated by the Supplier or Sub-contractor has in place appropriate technical and organisational measures to ensure that the Sub-contractor will store, access, manage and/or Process the Government Data as required by this Schedule 2 (*Security Management*); and
      2. the Supplier has provided the Buyer with such information as the Buyer requires concerning:
         1. the entity;
         2. the arrangements with the entity; and
         3. the entity’s compliance with the binding agreement; and
      3. the Buyer has not given the Supplier a Prohibition Notice under paragraph 1.3.
  1. Where the Supplier cannot comply with one or more of the requirements of paragraph 1.1:
     1. it must provide the Buyer with such information as the Buyer requests concerning the security controls in places at the relevant location or locations; and
     2. the Buyer may grant approval to use that location or those locations, and that approval may include conditions; and
     3. if the Buyer does not grant permission to use that location or those locations, the Supplier must cease to store, access or process Buyer Data at that location or those locations within such period as the Buyer may specify.
  2. The Buyer may by notice in writing at any time give notice to the Supplier that it and its Sub-contractors must not undertake or permit to be undertaken, the storage, access or Processing Buyer Data as specified in the notice (a “**Prohibited Activity**”).
     1. in any particular country or group of countries;
     2. in or using facilities operated by any particular entity or group of entities; or
     3. in or using any particular facility or group of facilities, whether operated by the Supplier, a Sub-contractor or a third-party entity (a “**Prohibition Notice**”).
  3. Where the Supplier or Sub-contractor, on the date of the Prohibition Notice undertakes any Relevant Activities affected by the notice, the Supplier must, and must procure that Sub-contractors, cease to undertake that Prohibited Activity within 40 Working Days of the date of the Prohibition Notice.

1. **Vetting, Training and Staff Access**

**Vetting before performing or managing Services**

* 1. The Supplier must not engage Supplier Personnel, and must ensure that Sub-contractors do not engage Sub-contractor Personnel, in any activity relating to the performance and management of the Services unless:
     1. That individual has passed the security checks listed in paragraph 2.2; or
     2. The Buyer has given prior written permission for a named individual to perform a specific role.
  2. For the purposes of paragraph 2.1, the security checks are:
     1. the checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:
        1. the individual’s identity;
        2. the individual’s nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;
        3. the individual’s previous employment history; and
        4. that the individual has no Relevant Convictions;
     2. national security vetting clearance to the level specified by the Buyer for such individuals or such roles as the Buyer may specify; or
     3. such other checks for the Supplier Personnel of Sub-contractors as the Buyer may specify.

**Annual training**

* 1. The Supplier must ensure, and ensure that Sub-contractors ensure, that all Supplier Personnel, complete and pass security training at least once every calendar year that covers:
     1. general training concerning security and data handling; and
     2. phishing, including the dangers from ransomware and other malware.

**Staff access**

* 1. The Supplier must ensure, and ensure that Sub-contractors ensure, that individual Supplier Personnel can access only the Buyer Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.
  2. The Supplier must ensure, and ensure that Sub-contractors ensure, that where individual Supplier Personnel no longer require access to the Buyer Data or any part of the Buyer Data, their access to the Buyer Data or that part of the Buyer Data is revoked immediately when their requirement to access Buyer Data ceases.
  3. Where requested by the Buyer, the Supplier must remove, and must ensure that Sub-contractors remove, an individual Supplier Personnel’s access to the Buyer Data or part of that Buyer Data specified by the Buyer as soon as practicable and in any event within 24 hours of the request.

**Exception for certain Sub-contractors**

* 1. Where the Supplier considers it cannot ensure that a Sub-contractors will undertake the relevant security checks on any Sub-contractor Personnel, it must:
     1. as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;
     2. provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Supplier Personnel will perform as the Buyer reasonably requires; and
     3. comply, at the Supplier’s cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Personnel and the management of the Sub-contractor.

1. **Security Testing**
   1. This paragraph applies only where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.
   2. **Note:** the definition of Supplier Information Management System includes those information and communications technology systems that Sub-contractors will use to assist or contribute to the Supplier providing the Services.
   3. The Supplier must, at the Buyer’s option, before providing the Services and when reasonably requested by the Buyer, either:
      1. conduct security testing of the Supplier Information Management System by:
         1. engaging a CHECK Service Provider or a CREST Service Provider;
         2. designing and implementing the testing so as to minimise its impact on the Supplier Information Management System and the delivery of the Services; and
         3. providing the Buyer with a full, unedited and unredacted copy of the testing report without delay and in any event within ten Working Days of its receipt by the Supplier; or
      2. Provide details of any security testing undertaken by a CHECK Service Provider or a CREST Service Provider in respect of the Supplier Information Management System in the calendar year immediately preceding the Buyer’s request or the Effective Date (as appropriate), including:
         1. the parts of the Supplier Information Management System tested;
         2. a full, unedited and unredacted copy of the testing report; and
         3. the remediation plan prepared by the Supplier to address any vulnerabilities disclosed by the security testing; and
         4. the Supplier’s progress in implementing that remediation plan.
   4. The Supplier must remediate any vulnerabilities classified as “medium” or above in the security testing:
      1. before Processing Buyer data where the vulnerability is discovered before the Supplier begins to process Authority Data;
      2. where the vulnerability is discovered when the Supplier has begun to Process Buyer Data:
         1. by the date agreed with the Buyer; or
         2. where no such agreement is reached:
            1. within five Working Days of becoming aware of the vulnerability and its classification where the vulnerability is classified as critical;
            2. within one month of becoming aware of the vulnerability and its classification where the vulnerability is classified as high; and
            3. within three months of becoming aware of the vulnerability and its classification where the vulnerability is classified as medium.
2. **End-user Devices**
   1. The Supplier must manage, and must ensure that all Sub-contractors manage, all End-user Devices on which Buyer Data is stored or processed in accordance the following requirements:
      1. the operating system and any applications that store, process or have access to Buyer Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;
      2. users must authenticate before gaining access;
      3. all Buyer Data must be encrypted using a encryption tool agreed to by the Buyer;
      4. the End-user Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;
      5. the End-user Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Buyer Data;
      6. the Suppler or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Buyer Data on the device and prevent any user or group of users from accessing the device;
      7. all End-user Devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any ISO/IEC 27001:2018 certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.
   2. The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Agreement.
   3. Where there any conflict between the requirements of this Schedule [x] (Security Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.
3. **Encryption**
   1. Unless paragraph 5.2 applies, the Supplier must ensure, and must ensure that all Sub-contractors ensure, that Buyer Data is encrypted:
      1. when stored at any time when no operation is being performed on it; and
      2. when transmitted.
   2. Where the Supplier, or a Sub-contractor, cannot encrypt Buyer Data as required by paragraph 5.1, the Supplier must:
      1. immediately inform the Buyer of the subset or subsets of Buyer Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
      2. provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption;
      3. provide the Buyer with such information relating to the Buyer Data concerned, the reasons why that Buyer Data cannot be encrypted and the proposed protective measures as the Buyer may require.
   3. The Buyer, the Supplier and, where the Buyer requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Buyer Data.
   4. This paragraph applies where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.
   5. Where the Buyer and Supplier reach agreement, the Supplier must update the Security Management Plan to include:
      1. the subset or subsets of Buyer Data not encrypted and the circumstances in which that will occur;
      2. the protective measure that the Supplier and/or Sub-contractor will put in please in respect of the unencrypted Buyer Data.
   6. Where the Buyer and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Buyer Data, either party may refer the matter to anna.brostromer@cabinetoffice.gov.uk
4. **Access Control**
   1. The Supplier must, and must ensure that all Sub-contractors:
      1. identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;
      2. require multi-factor authentication for all user accounts that have access to Buyer Data or that are Privileged Users;
      3. allow access only to those parts of the Supplier Information Management System and Sites that those persons require;
      4. maintain records detailing each person’s access to the Supplier Information Management System and Sites, and make those records available to the Buyer on request.
   2. The Supplier must ensure, and must ensure that all Sub-contractors ensure, that the user accounts for Privileged Users of the Supplier Information Management System:
      1. are accessible only from dedicated End-user Devices;
      2. are configured so that those accounts can only be used for system administration tasks;
      3. require passwords with high complexity that are changed regularly;
      4. automatically log the user out of the Supplier Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive.
   3. The Supplier must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different passwords for their different accounts on the Supplier Information Management System.
   4. The Supplier must, and must ensure that all Sub-contractors:
      1. configure any hardware that forms part of the Supplier Information Management System that is capable of requiring a password before it is accessed to require a password; and
      2. change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.
5. **Malicious Software**
   1. The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier Information Management System.
   2. The Supplier shall ensure that such Anti-virus Software:
      1. is configured to perform automatic software and definition updates;
      2. performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and
      3. where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.
   3. If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Buyer Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.
   4. Any cost arising out of the actions of the parties taken in compliance with the provisions of paragraph 7.3 shall be borne by the parties as follows:
      1. by the Supplier where the Malicious Software originates from the Supplier Software, any third-party software licenced by the Supplier or the Buyer Data (whilst the Buyer Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and
      2. by the Buyer, in any other circumstance.
6. **Breach of Security**
   1. If either party becomes aware of a Breach of Security it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within 24 hours.
   2. The Supplier must, upon becoming aware of a Breach of Security or attempted Breach of Security immediately take those steps identified in the Security Management Plan (if applicable) and all other reasonably steps necessary to:
      1. minimise the extent of actual or potential harm caused by such Breach of Security;
      2. remedy such Breach of Security to the extent possible;
      3. apply a tested mitigation against any such Breach of Security; and
      4. prevent a further Breach of Security in the future which exploits the same root cause failure.
   3. As soon as reasonably practicable and, in any event, within five Working Days, or such other period agreed with the Buyer, following the Breach of Security or attempted Breach of Security, provide to the Buyer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.
   4. The Supplier must take the steps required by paragraph 8.2 at its own cost and expense.
7. **Sub-contractors**
   1. The Supplier must assess the parts of the information and communications technology system and the Sites that its Sub-contractors will use to provide the Services against the NCSC Cloud Security Principles at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-contractor must document that assessment and make that documentation available to the Buyer at the Buyer’s request.
8. **Third-party Software**
   1. The Supplier must not, and must ensure that Sub-contractors do not, use any software to Process Buyer Data where the licence terms of that software purport to grant the licensor rights to Progress the Buyer Data greater than those rights strictly necessary for the use of the software.
9. **Deletion of Buyer Data**
   1. The Supplier must, and must ensure that all Sub-contractors, securely erase any or all Buyer Data held by the Supplier or Sub-contractor when requested to do so by the Buyer using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.

Appendix 3

**Call-Off Schedule 14 (Service Levels)**

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

|  |  |
| --- | --- |
| “Critical Service Level Failure” | has the meaning given to it in the Order Form; |
| "Service Credits" | any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels; |
| "Service Credit Cap" | has the meaning given to it in the Order Form; |
| "Service Level Failure" | means a failure to meet the Service Level Performance Measure in respect of a Service Level; |
| "Service Level Performance Measure" | shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and |
| "Service Level Threshold" | shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule. |

1. **What happens if you don’t meet the Service Levels**
   1. The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.
   2. The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A of this Schedule including the right to any Service Credits and that any Service Credit 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 meet any Service Level Performance Measure.
   3. The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.
   4. A Service Credit shall be the Buyer’s exclusive financial remedy for a Service Level Failure except where:
      1. the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or
      2. the Service Level Failure:
         1. exceeds the relevant Service Level Threshold;
         2. has arisen due to a Prohibited Act or wilful Default by the Supplier;
         3. results in the corruption or loss of any Government Data; and/or
         4. results in the Buyer being required to make a compensation payment to one or more third parties; and/or
      3. the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).
   5. Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months’ notice, change the weighting of Service Level Performance Measure in respect of one or more Service Levels and the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:
      1. the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;
      2. the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards; and
      3. there is no change to the Service Credit Cap.
2. **Critical Service Level Failure**

On the occurrence of a Critical Service Level Failure:

* 1. any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and
  2. the Buyer shall (subject to the Service Credit Cap) be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period ("**Compensation for Critical Service Level Failure**"),

provided that the operation of this paragraph 3 shall be without prejudice to the right of the Buyer to terminate this Contract and/or to claim damages from the Supplier for material Default.

**Part A: Service Levels and Service Credits**

1. **Service Levels**

If the level of performance of the Supplier:

* 1. is likely to or fails to meet any Service Level Performance Measure; or
  2. is likely to cause or causes a Critical Service Failure to occur,

the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:

* + 1. require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;
    2. instruct the Supplier to comply with the Rectification Plan Process;
    3. if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or
    4. if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure (including the right to terminate for material Default).

1. **Service Credits**
   1. The Buyer shall use the Performance Monitoring Reports supplied by the Supplier to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.
   2. Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in the Annex to Part A of this Schedule.

**Annex A to Part A: Services Levels and Service Credits Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Service Level Performance Criterion | Key Indicator | Service Level Performance Measure | Service Level Minimum Threshold | Buyer redress for Failure to provide Services at or above Service Levels |
| Deliverable to meet agreed acceptance criteria, due date and Charges as set  out in the relevant  Statement of Work.  Service Level applies to all Statements of Work during the Call-Off Contract  Period. | Performance. | At least 90% achievement of all  Deliverables provided under all  Statements of Work will meet the  agreed acceptance criteria, due  date and Charges as set out in  the relevant Statement of Work.  Service Level Minimum Threshold will be calculated as a  percentage of the total  Deliverables that have met the agreed acceptance criteria, due date and Charges as set out in the relevant Statement of Work, during each rolling Month of the  Call-Off Contract Term. | Achieving less than 90%. | Once below the  Service Level Minimum Threshold, the Supplier will  engage with the Buyer to provide a formal plan to meet the Service Level Minimum Threshold,  subject to Joint Schedule 10 (Rectification Plan  Template).  Service Credits to be  notified to the Supplier by the Buyer with reasonable notice. |
| Supplier to resource the Services with appropriate Supplier Staff within 20 Working Days of the  relevant Statement of Work being executed.  All Supplier Staff must be appropriately trained and qualified, be vetted using Good Industry Practice and  the Security Policy, and comply with all conduct requirements when on the Buyer’s Premises. | Performance /  timelines. | Appropriate resourcing arranged within 20 Working Days of the  relevant Statement of Work being executed.  Service Level Minimum Threshold will be calculated as a  percentage of the total  Statements of Work that have been appropriately resourced within 20 Working Days, during  each rolling Month of the Call-Off Contract Term. | Achieving  less than 75%. | Once below the  Service Level Minimum Threshold, the Supplier will  engage with the Buyer to provide a formal plan to meet the Service Level  Minimum Threshold,  subject to Joint Schedule 10 (Rectification Plan  Template).  Service Credits to be  notified to the Supplier by the Buyer with reasonable notice. |
| Accurate and timely billing by the Supplier, as required by Call-Off  Schedule 5 (Pricing  Details). | Accuracy /  Timelines. | At least 95% of the Invoices must be raised in an accurate  and in a timely way, in accordance with Call-Off Schedule 5 (Pricing Details).  Service Level Minimum Threshold will be calculated as a  percentage of the total Invoices that have been raised in an  accurate and timely way, in accordance with Call-Off Schedule 5 (Pricing Details),during each rolling Month of the  Call-Off Contract Term. | Achieving  less than 95%. | Once below the  Service Level Minimum Threshold, the Supplier will  engage with the Buyer to provide a formal plan to meet the Service Level  Minimum Threshold,  subject to Joint Schedule 10 (Rectification Plan  Template).  Service Credits to be  notified to the Supplier by the Buyer with reasonable notice. |

The Service Credits relating to these Service Levels and the formula by which such Service Credits shall be calculated will be notified to the Supplier by the Buyer with reasonable notice before such Service Levels are implemented.

**Part B: Performance Monitoring**

1. **Performance Monitoring and Performance Review**
   1. Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.
   2. The Supplier shall provide the Buyer with performance monitoring reports ("**Performance Monitoring Reports**") in accordance with the process and timescales agreed pursuant to paragraph 1.1 of Part B of this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:
      1. for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;
      2. a summary of all failures to achieve Service Levels that occurred during that Service Period;
      3. details of any Critical Service Level Failures;
      4. for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;
      5. the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and
      6. such other details as the Buyer may reasonably require from time to time.
   3. The Parties shall attend meetings to discuss Performance Monitoring Reports ("**Performance Review Meetings**") on a Monthly basis. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:
      1. take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location and time (within normal business hours) as the Buyer shall reasonably require;
      2. be attended by the Supplier's Representative and the Buyer’s Representative; and
      3. be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Buyer’s Representative and any other recipients agreed at the relevant meeting.
   4. The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Supplier's Representative and the Buyer’s Representative at each meeting.
   5. The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

**Appendix 4**

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

**REDACTED TEXT under FOIA Section 43 Commercial Interests**

Appendix 5

**Call-Off Schedule 5 (Pricing Details)**

**Part A: Charges**

1. **Call-Off Charges**
   1. The Charges shall be calculated in accordance with the terms of the Call-Off Contract and in particular in accordance with the Order Form and this Call-Off Schedule 5 (Pricing Details) and shall be the full and exclusive remuneration of the Supplier in respect of the performance of the Services.
   2. The Charges for any Deliverables and/or Services provided under any Statement of Work shall be set out in such relevant Statement of Work. Unless otherwise agreed in writing by the Supplier, the Charges shall include every cost and expense of the Supplier directly or indirectly incurred in connection with the performance of the Services.
   3. The Charges shall be calculated in accordance with the day rates set out in the rate card annexed to this Call-Off Schedule 5 (Pricing Details) and any of the following charging bases, as requested by the Buyer:
      1. Fixed

Where the Buyer and the Supplier agree a fixed price (covering all necessary costs for the Deliverables). The Supplier will continue at its own cost to provide the Deliverables where the agreed fixed price has been exceeded, and the Buyer will pay the agreed fixed price only. The Buyer will have no obligation or liability to pay for the cost of any Deliverables delivered relating to the relevant Statement of Work after the agreed price has been exceeded.

* + 1. Time and Materials

Where the Buyer pays a total cost (covering all necessary costs for the Deliverables), calculated on the basis of the Supplier’s day rates for the total number of days required to deliver the Deliverables as set out in the relevant Statement of Work.

* + 1. Capped Time and Materials

Where the Buyer and the Supplier agree a maximum total cost (covering all necessary costs for the Deliverables), calculated on the basis of the Supplier’s day rates for the total number of days required to deliver the Deliverables as set out in the relevant Statement of Work. The Supplier will continue at its own cost to provide the Deliverables where the agreed maximum total cost has been exceeded, and the Buyer will pay the maximum total cost only. The Buyer will have no obligation or liability to pay for the cost of any Deliverables delivered relating to the relevant Statement of Work after the agreed price has been exceeded. If the Supplier delivers the Deliverables early, the Buyer shall only pay the Supplier for the time taken to deliver the Deliverables.

1. **Changes to the Charges**
   1. The Charges will be fixed in accordance with Paragraph 4 of Framework Schedule 3 (Framework Prices). For the avoidance of doubt, the Charges shall not be impacted by any change to the Framework Prices.
   2. Without prejudice to the terms set out in Paragraph 4 of Framework Schedule 3 (Framework Prices) relating to the Framework Prices, the Charges may also be varied due to:
   3. in respect of all Charges, any of the reasons set out in Paragraph 5.1 of Framework Schedule 3 (Framework Prices); and

**Part B: Payment Terms**

1. **General Payment Terms** 
   1. The Charges levied in accordance with this Schedule, less any Delay Payments, shall be the Supplier’s entire remuneration under this Call-Off Contract.
   2. The terms of Clause 4 of the Core Terms (version 3.0.10) for RM6193 apply to the Charges.
   3. A Supplier invoice is only valid if it:
      1. complies with the terms of clause 4.5 of the Core Terms (version 3.0.10) for RM6193; and
      2. provides a full itemisation of the Charges, quoting the relevant SOW Number(s) against the relevant Charges for each Statement of Work that is being invoiced.
   4. If the Buyer disputes any invoice:
      1. the Buyer shall notify the Supplier in writing within 5 days of the date of receipt of the invoice, specifying the reasons for disputing the invoice;
      2. the Supplier shall provide all evidence as may be reasonably necessary to verify the disputed invoice;
      3. the Buyer shall pay to the Supplier all amounts not disputed by the Buyer on the due date as set out in Clause 4 of the Core Terms (version 3.0.10) for RM6193;
      4. the Parties shall negotiate in good faith to attempt to resolve the dispute promptly; and
      5. if the parties have not resolved the dispute within 30 days of the Buyer giving notice to the Supplier, the dispute shall be resolved in accordance with Clause 34 in CCS Core Terms (version 3.0.10) for RM6193.
      6. The Buyer may retain or set-off payment of any amount owed to it by the Supplier if notice and reasons are provided as set out in Paragraph 6 (in respect of Services other than Support and Maintenance Services) of this Call-Off Schedule 5 (Pricing Details).
      7. The Supplier has no right of set-off, counterclaim, discount or abatement unless they are ordered to do so by a court.
2. **Payment terms for all Charges payable in respect of Services other than fixed price elements**
   1. For Services other than those relating to Support and Maintenance Services or as otherwise agreed by the Parties, the Supplier shall issue invoices to the Buyer at the end of each month for the relevant pro-rata portion of the Charges set out in the relevant Statements of Work.
   2. The payment of each SOW shall be conditional on the Statement of Work reaching Full Achievement.
   3. A Statement of Work shall be deemed to have reached Full Achievement when all Deliverables under the relevant Statement of Work have:
      1. been delivered to the reasonable satisfaction of the Buyer; and
      2. met the corresponding acceptance criteria and the Buyer has confirmed in writing to the Supplier that the relevant Statement of Work has been completed to the Buyer’s reasonable satisfaction.

**Pricing**

**REDACTED TEXT under FOIA Section 43 Commercial Interests**

Appendix 6

**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

# PURPOSE

## The Cabinet Office requires a three (3) year Managed and Professional Services contract, on a call-off basis, to provide specialist Enterprise Resource Planning (ERP) technical client-side support for departmental-level responsibilities within our cross-government policy cluster (Matrix Portfolio) programme.

## The Authority expects this service to provide us with a key set of products and the assurance that our Cluster-level System Implementation (SI) partner’s configuration of the IT will deliver the outcomes we require to our functional and technical specifications.

## The purpose of our forthcoming further competition is to seek client side specialist ERP (Workday) technical support for Cabinet Office for the design, build and test phases of the Matrix programme through to the launch of the technical solution and post go live.

# BACKGROUND TO THE CONTRACTING AUTHORITY

## The Cabinet Office is a central government department of the United Kingdom, which is responsible for supporting the prime minister and Cabinet. Cabinet Office forms the corporate headquarters for government, in partnership with HM Treasury, and takes the lead in certain critical policy areas. It is composed of various units that support Cabinet committees and which coordinate the delivery of government objectives via other departments ensuring all Departments are able to deliver on the Prime Minister’s ambition.

# BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

## The findings of the Internal Maude review into Shared Services (March 2021), led to a revised Shared Services Strategy for Government. This revised strategy saw the formation of five departmental clusters and alignment on technology and strategic direction, which removed the individual sourcing approach which was being conducted by the majority of departments.

## As one of the nine departments forming the ‘Matrix’ Cluster, we are now working on a collaborative solution to meet our joint Software as a Service (SaaS) Enterprise Resource Planning system and Business Process Outsource support needs, and therefore need to ensure Cabinet Office receives an optimal solution to drive better Corporate Services for its approx 10,000 system users.

* 1. We intend to consider and take account of all relevant social value themes and outcomes throughout our procurement, including:
* The minimising of any potential environmental impacts of undertaking this project
* Tackling regional workforce inequality in the delivery of this project
* How the health and wellbeing of those actively deployed onto the project will be monitored and managed

# DEFINITIONS

|  |  |
| --- | --- |
| EXPRESSION OR ACRONYM | DEFINITION |
| ERP | ENTERPRISE RESOURCE PLANNING |
| SI | SYSTEM IMPLEMENTER |
| SPADs | SPECIAL ADVISORS. |
| SaaS | SOFTWARE AS A SERVICE. |
| CO | CABINET OFFICE |
| MyCO | CABINET OFFICE - PROGRAMME TEAM |
| SOP | SINGLE OPERATING PLATFORM |
| BPO | BUSINESS PROCESS OUTSOURCE |
| MATRIX | SHARED SERVICES ‘POLICY’ CLUSTER/ PROGRAMME (INCL DSIT, DESNZ, CABINET OFFICE, DCMS, DBT, HMT, DFE, DHSC AND AGO) |

# SCOPE OF REQUIREMENT

## A system implementation partner has now been procured by the Matrix Programme team to deliver a new Workday SaaS ERP system for all nine departments within the Matrix Cluster.

## As we enter the detailed design stage of the programme we require Client-side support to ‘face off’ to Matrix Central Team and the newly procured SI Partner through completion of a set of key deliverables which will help ensure all Cabinet Office department project responsibilities are completed to plan and our list of requirements, which essentially forms the blueprint of our system and process needs, is delivered to our satisfaction

## The chosen Supplier will execute deliverables by engaging with internal Cabinet Office stakeholders as well as the Matrix programme team as appropriate, to ensure critical design and build activities are completed to Cabinet Office’s requirements.

## These activities and outputs will require pacey decision making and sensitive stakeholder engagement, ensuring the Matrix system is being developed with the SI Partner to meet our requirements, and that Cabinet Office stakeholders (Subject Matter Expert’s & Process Owners) understand and are content with the Matrix solution being developed by the SI Partner.

## The current timeline for Cabinet Office to onboard to the new system is expected to be around June 2026. Detailed design and build stages are expected to run throughout the majority of 2025 as we will then move into testing phase towards the end of the year and start cutover works in early 2026 for onboard around June the same year.

## As this is a very complex multiple department programme led by the Department for Science Innovation and Technology, we only have a detailed plan (for what this means for Cabinet Office as the first mover department) at present for design and build phases. To ensure we have the necessary core support throughout the detailed design and build phase of the programme, we will be seeking a fixed price from suppliers for continued support throughout this extremely key programme phase. In addition to this we will be seeking average rate card costs so that we can draw down through ‘statements of work' additional/ further specialist related support for the latter parts of the programme when our understanding of what we need to do as a department in the Matrix Cluster becomes clearer.

# THE REQUIREMENT

## Provision of a 3 year call off contract (framed as 2 Years + 1 year) that will be used by the Supplier to provide a series of key products ‘on the client side’ against our programme plan and provide the MyCO Programme with the necessary assurance that CO ERP system, process needs and requirements are being optimally met.

## To assist with the move from our legacy SOP ERP (On premise Oracle based system) to a new Cloud based Workday ERP the Supplier should have knowledge and previous experience, training or certification in Oracle and Workday ERP technologies. The Supplier will be expected to provide expert services to cover the following functional and non functional areas to support our move to Workday Cloud ERP, as set out in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| Deliverables | Products | Indicative Dates | |
| From | To |
| Technology Design | | | |
| Assure security postures for the Matrix solution align with Cabinet Office security policies and overall Matrix compliance requirements. | Ensure Cabinet Office security approval of the security posture and hosting of the Matrix solution ensuring compliance with the NCSC 14 Cloud Adoption Security Principles throughout Architecture & Configure phase | Feb 25 | Oct 25 |
| Assure and act as the technical expert / advisor on the alignment of Matrix solution config and build to Cabinet Office Systems ensuring the end solution meets Cabinet Office requirements | Develop a technology roadmap of relevant components of the Matrix solution and their relevance to Cabinet Office Technical Design Authority and providing regular assurance updates to MyCO Delivery Board throughout Architecture & Configure phase | Feb 25 | Oct 25 |
| Continually monitoring the SI plan and ensuring requirements in which Cabinet Office input is needed, is both feasible and achievable in timeframes specified, ensuring collaborative build for the Matrix system is achieved in a timely manner. | Regular assurance reports with Risk register delivered to the MyCO Programme Board and CO Digital Technical Design Authority throughout Architecture & Configure phase | Feb 25 | Oct 25 |
| Assure system configuration through the prototyping and build to ensure the new Matrix system meets Cabinet Office requirements. | Assurance reports to MyCO Delivery Board and/ or CO Digital Technical Design Authority | Feb 25 | Oct 25 |
| Align Technology outputs to review integration specifications, coordinate business input into integration specifications. | Ongoing review and input to Matrix Architecture and Integrations 3 wave worksets providing assurance to MyCO Delivery Board and CO Digital Technical Design Authority to sign off for Matrix Tech Integrations workbooks | Feb 25 | Oct 25 |
| Functional Design: Covering HR, Finance, Payroll and Reporting | | | |
| Utilise Matrix governance forums to gain assurance that any Cabinet Office exceptions to the adopt not adapt principle have been validated and approved by all parties prior to inclusion by the SI in the solution | Support stakeholders during iterative playback sessions and provide system demonstrations and walkthroughs of functionality, process maps etc providing them with the assurance that each process meets our functional needs. | Feb 25 | Oct 25 |
| Assure and Act as the Cabinet Office technical expert / advisor on HR, Finance, Payroll and Reporting l design, | Provide ongoing support through Detailed designs and Architecture & Configure phases, providing impact assessments, written and verbal updates, ensuring traceability of decision making and alignment of work to future benefits. Document key processes for divergent business areas to ensure all requirements are met, working alongside service design colleagues to ensure the end to end solution delivers Cabinet Office needs. | Feb 25 | Oct 25 |
| Assure Matrix Cross Functional Design and guidance for Cabinet Office on the impact of the design and build on user experience, process architecture, workflows and digital assistance | Ongoing review and assurance throughout detailed design and Architecture and Configure phase, providing assurance reports and Impact assessments for CO Governance, MyCO Delivery Board and CSTP. | Feb 25 | Oct 25 |
| Provide Functional Solution Architecture oversight ensuring coherence of design and strategic design intent meets Cabinet Office requirements and vision (working with our SME’s and Process Owners). | Ongoing review and assurance throughout detailed design and Architecture and Configure phase, providing assurance reports and Impact assessments for CO Governance, MyCO Delivery Board and CSTP. | Feb 25 | Oct 25 |
| Policy Harmonisation and Convergence:  Provide specialised support for Cabinet Office SME’s & Process Owners in Matrix harmonisation and convergence of policies and processes across functional and service workstreams | Monitor outputs and support Cabinet Office SME’s during Matrix Policy Harmonisation and Convergence workshops, Provide Cabinet Office design insights and expertise to inform and support policy re-drafting and documentation updates. | Feb 25 | Oct 25 |
| Work with Matrix Cluster, to ensure alignment of technology/ functional activity with service colleagues to ensure the end to end system and service offering meets Cabinet Office needs. | Ongoing consideration in order to ensure overall solution developed meets end to end of Cabinet Office, providing verbal updates, assurance reports and impact assessments. | Feb 25 | Oct 25 |
| Specifically in Reporting design: | | | |
| Understand the functional reporting outcomes aligned to each element of the taxonomy for e2e process including service. | Agree a set of reporting requirements that can be used to drive creation of reporting specifications and Matrix SI’s understanding of our reporting outcomes from the system. | Feb 25 | Oct 25 |
| Understand the service reporting outcomes aligned to each element of the taxonomy to allow performance management from a BPO. | Agree on a set of reporting requirements that can be used to drive creation of reporting specifications and Matrix SI’s understanding of our reporting outcomes from the system. | Feb 25 | Oct 25 |
| Business Change & Engagement: | | | |
| Work with Cabinet Office Business Units to develop localised plans in order to prepare our department and stakeholders for the technology change ahead and how that will impact on their future ways of working. | * Transition and readiness plans * Readiness checklist * Ensuring Key networks are established | June 25 | Oct 25 |
| Ensure Matrix training needs strategy and plan works for Cabinet Office, review and assure the central approach, identifying impacts on Cabinet Office plans. With special impetus on Identifying and articulating the training needs of the multiple impacted and divergent groups in Cabinet Office and then reflect this in localised transition plans. | * Detailed Training Approach | Feb 25 | May 25 |
| Develop a training strategy and formulate a training delivery plan, providing oversight of delivery with a view to ensuring the effectiveness e.g CO staff receive appropriate, accessible and timely training and/or guidance, which will enable all Cabinet Office levels of users to fully utilise the new cloud based Workday ERP technology. | * Departmental Specific Training Plan (incorporating the needs of approximately 37 business units) | Feb 25 | June 25 |
| Complete Training Needs Analysis to determine the different levels and types of training Cabinet Office users will need in order to improve their job performance. | * Training needs analysis | Feb 25 | Aug 25 |
| Change analysis - To include the management and analysis of very high volumes of change related data, with varying levels of complexity | * Change impact assessments (approx 37 Business units) | Feb 25 | Oct 25 |
| Define and develop training plan for each persona and BU Identify and upskill trainers and also identify and consider any accessibility requirements. | * Work with SI training outputs in order to ensure relevance and accuracy, to support any divergence for ‘train the trainers’ sessions and training collateral | Aug 25 | Oct 25 |
| Data Migration | | | |
| Coordinate the execution of each data extraction required for Matrix data migration cycle (DM1-DM4) ensuring testing and reconciliation are achieved (approx 4 cycles over the next 8 months, there will be more but additional cycles will be drawn down via ‘SoW’ when plans are clearer) | Production of extraction files passed to Matrix SI Partner  Signed off extraction reconciliations by SSCL and validated by Cabinet Office SME’s. Validate load reconciliations that match source through SSCL and Cabinet Office SME’s. Providing validation reports for each cycle at a summary level for MyCO Programme Board | Feb 25 | Oct 25 |
| Work with Cabinet Office current BPS supplier (SSCL) to develop the data migration extraction procedures resolving conflicts between and the Matrix System Implementer | Maintain a set of version controlled specifications with an associated change control procedure which ensures Cabinet Office can meet its responsibilities to the Matrix Programme whilst ensuring a cost effective usage of SSCL resources | Feb 25 | Oct 25 |
| Completion and approvals through internal governance of DPIA’s before any sharing of our data with the Matrix team and/ or the Matrix System Implementation Partner | Completion of DPIA’s and ensure any/ all related Security assurance processes (incl GDPR) are met - assurance reports to MyCO Delivery Board and CO Data Board | Feb 25 | Oct 25 |
| Establish, assure and implement with Cabinet Office Digital the data transit method from SSCL to the Matrix System Implementer's data transformation staging area | Create and formulate a 'Pipeline' in order to share/ send data from CO to Matrix partners. | Feb 25 | Oct 25 |

## Our requirements consist of a series of working products to ensure the technical and specialised ERP outputs developed by the Matrix Cluster, are aligned to the Cabinet Office’s requirements and to ensure our business readiness for system and service transition.

## The fixed price work packages throughout the detailed design and build phase will involve translating requirements and configuration into an understanding of new ways of working, ensuring Matrix SI proposals meet our departmental needs and assessing their impacts, so that we can prepare our business for the changes ahead and ensure that as a department we get the most optimal solutions for our new technology.

## Our core requirements throughout the Matrix Programme Design & Build phase for which we will be seeking a fixed price are split across 7 key workstreams:

* + 1. Technology;
    2. Functional HR;
    3. Functional Finance;
    4. Functional Payroll;
    5. Functional Reporting;
    6. Change & Engagement; and
    7. Data Migration (including cleanse)

## 

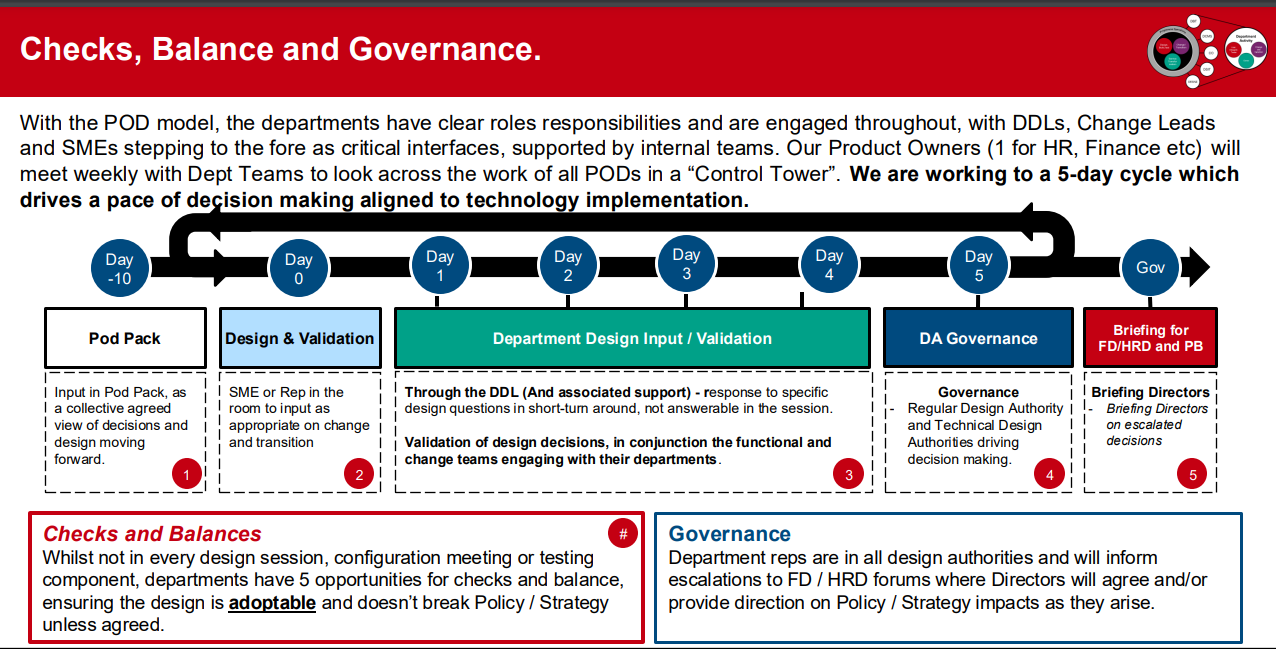
## The scope of this work will span approx c30 process areas across HR, Finance and Payroll. Through internal Matrix workshops, blueprinting and our Design & Change Authority, Cabinet Office has identified around c30 process areas and below them lay approx 3,000 ERP system, process and implementation requirements (Across Functional, Non Functional and Cross Functional areas as outlined in the below table).

|  |  |  |
| --- | --- | --- |
| HR | Finance | Cross or Non-functional |
| * Onboarding & Offboarding * Employee details/changes * Global mobility * Manage organisation and positions * Recruitment * Contingent and other types of workers * Absence, health and wellbeing, manage time * Reward * Payroll * Learning and development * Employee engagement * Manage performance, conduct & discipline, talent and succession | * S2C Purchase to pay * Expenses * Tax * Grants administration * Order to cash * Cash management * NCA (Assets) * Record 2 Report x3 | * Data * Data archive * Reporting * Integrations * Security * ServiceNow/Case management * Change and training * People Experience & Enabling Services * R2R, HR Strategic Planning, Workforce Planning * Optional components - Time tracking, project accounting, recruiting, inventory |

## Context - Detailed Design (Gap Analysis & Common Design)

## Support for the detailed design of the ERP solution within approx 30 functional process areas across HR, finance and payroll will be delivered using an agile workshop format running on 5 day cycles to take key detailed design decisions on the build of the ERP system. The process aims to sign-off decisions at the end of each week or if necessary to escalate to departmental governance. The key focus will be on driving a pace of decision making using an ‘adopt not adapt’ principle..

## An illustration of the (POD Model) detailed design process is provided below:

  
  
Functional support will be required to provide additional knowledge and expertise, in conjunction with Cabinet Office HR and Finance SMEs within these 5 day workshops. This will include facilitating Cabinet Office departmental responses to specific design questions in short-turn around, not answerable in the session. ​It will also include validation of design packs, in conjunction with change teams via engaging with their departments.

* 1. Specifically this will also include:

SME Engagement on final design ensuring validation​

Mapping of the business impact into the departmental CIA and necessary transition / change activities​

Updates to training needs analysis per process area (as required)​

Managing the internal change landscape to de-risk delivery and optimise change activity;

## Context - Build (Architecture & Configure)

* 1. As per the current plan, running in sequence with Detailed Design (Common Design/ Gap Analysis) will be the Build (Architecture and Configuration) phase. This phase will require providing Cabinet Office expertise and ERP development input into three work sets over an approx 30 day period each with the Matrix System Implementor, these worksets will include:

From a functional perspective, per workset cycle:

* + 1. Design Sessions - covering all workstreams (approx 10 days)
    2. Workset Configuration Workbooks Completed (All HCM, All FINS , Payroll) (approx 10 days)
    3. Workset Enhancements to Reporting Tracker (approx 11 days)
    4. Design Follow up & Configuration: Update (approx 10 days)
    5. Playback: Review & Validate Build Increment / Configuration (All HCM, All FINS , Payroll) (approx 10 days)
    6. Agreement to proceed to workset C (soft sign off) - All HCM, All FINS , Payroll (approx 10 days)
    7. Reflection / Review Week (approx 5 days)

Reporting - over the the full workset cycle:

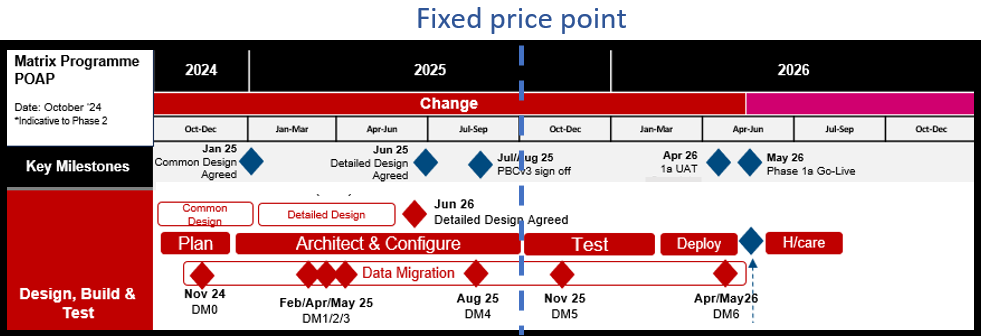
* + 1. Detailed Design and Build commences (Workset 1,2,&3 over approx 76 days)
    2. Report Playback (iterative over approx 60 days)

Technology Integrations perspective, per workset cycle:

* + 1. Batch Integrations - Requirements gathering discussions with Business / Discovery / Design (approx 25 days)
    2. Batch Integrations - Low Level Design (approx 25 days)
    3. Batch Integrations - Build Phase (approx 28 days)
    4. Batch Integrations - Integrations Connectivity Test (Approx 10 days)
    5. Batch Integrations System & Connectivity Test

Data Perspective, per workset cycle:

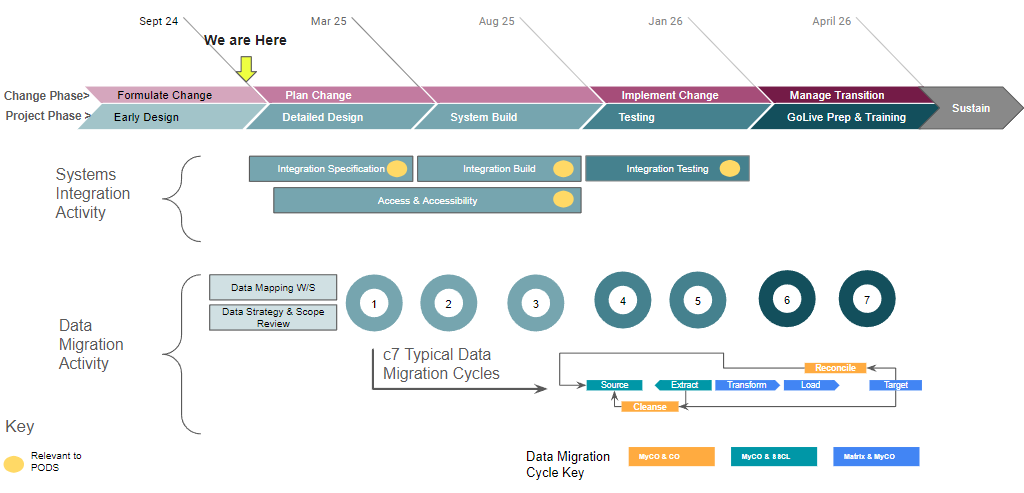
* + 1. Workset Data Load (approx. 5 days)
    2. Workset Data subset - Extract (Timeline TBC – approx. 12 days)
    3. Workset Data subset – Transform (approx 11 days)
    4. Workset Initial Data Submission (approx 1 day)
    5. Workset Data Validation (approx 5 days)
    6. Workset A Final Data Submission (1 day)
    7. Please see below Data illustration (6.15 & 6.17) Fixed price data support is required for DM1-4.
  1. Business Change and Engagement work will run alongside the above activities as per the below timeline providing valuable expertise in defining and developing training approach, strategy, planning and the development of bespoke training materials/ collateral providing valuable support for Cabinet Office staff on the way in which we will work in future as set out in the deliverables table
  2. The below table sets out the indicative timeline for Cabinet Office Go- Live in May/June 2026 and we are seeking a fixed price for the above listed specialist support up until the end of October (close of Architecture & Configure phase).



## Following the successful delivery of the first phase deliverables outlined above (to the end of Architect and Configure), outcomes will be delivered for the remainder of the contract in the Testing, Deploy/ Cutover and Hypercare phases, BAU support for our transition from Oracle and any interim improvements to our current (Oracle) system via a Statement of Works mechanism. Deliverables are likely to fall within the scope of the seven major work stream areas outlined below:

* + 1. Technology;
    2. Functional HR;
    3. Functional Finance;
    4. Functional Payroll;
    5. Functional Reporting;
    6. Change & Engagement; and

## Data Migration (including cleanse - detailed illustration below)



## The parties will execute a SoW Form for each work package, which will include specific details of outcomes required under that SoW as well as details of location and specific service level agreements, performance measures and KPIs in regard to that specific SoW.

## All roles provided under any SoW Form issued under this Contract will be mapped back to SFIA Grades 3 to 7 inclusive. The sole exception to this may be any Apprentices or trainees who are provided at the Supplier’s cost, who may be SFIA Grade 1 or 2.

# KEY MILESTONES AND DELIVERABLES

## In the above table within section 6 we have set our key deliverables and provided an indicative timeframe for when we expect each piece of work will be required. This timeline is based on our current outline Matrix plans, however changes to plans or the sequencing of work should not affect the cost of the work as long as the deliverables are still within the 3 year contracting period.

# 

# MANAGEMENT INFORMATION/REPORTING

* 1. The Supplier will be expected to provide weekly progress updates to workstream leads during weekly team meetings and also provide a monthly progress update during supplier performance meetings with the Programme Manager and Workstream leads.
  2. The Supplier shall provide Management Information in regards to:
     1. Within two weeks of commencement a detailed delivery plan for the fixed price package for all seven workstreams throughout the design and build phases;
     2. Weekly updates for work packages and deliverables currently being undertaken;
     3. Engagement dates;
     4. Cost to date; and
     5. Cost forecasting.

# VOLUMES

## The Supplier shall be able to deal with large volumes immediately from the contract commencement date and shall have capacity to enrol, contact and allocate a programme tutor at the point of receipt.

# CONTINUOUS IMPROVEMENT

## The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

## The Supplier should present new ways of working to the Authority during monthly Contract review meetings.

## Changes to the way in which the Services are to be delivered must be brought to the Authority’s attention and agreed prior to any changes being implemented.

# SUSTAINABILITY

## The suppliers will provide evidence that they operate a paperless process in how they conduct their business.

## Working remotely where it is feasible to do so, should be considered to reduce unnecessary travel.

# QUALITY

## To ensure a consistent approach and quality is achieved, all project deliverables must be peer reviewed by a member of the MyCO Programme and agreed with the relevant subject matter experts within the business reference group and design & change authority.

## We will also be undertaking quarterly evaluation of performance with Departmental SME’s and central Matrix colleagues in order to assist with measuring supplier satisfaction with the services being delivered

# PRICE

## Prices are to be submitted via the e-Sourcing Suite Attachment 4 – Price Schedule excluding VAT and including all other expenses relating to Contract delivery.

## The maximum budget available for this requirement is £6m (ex VAT).

## Pricing should be based on total net cost (ex VAT) for each of the required deliverables as set out in section 7.

# STAFF AND CUSTOMER SERVICE

## The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.

## The Supplier’s staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

## The Supplier shall ensure that staff understand the Authority’s vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.

## SERVICE LEVELS AND PERFORMANCE

## The Authority will measure the quality of the Supplier’s delivery by:

# 

|  |  |  |  |
| --- | --- | --- | --- |
| KPI | SERVICE AREA | KPI/SLA DESCRIPTION | TARGET |
| 1 | Turnaround Time | The Supplier will provide profiles of operatives within 5 working days of Customer request and be ready to mobilise within 10 working days of signed SoW | No more than 1 instance of non-compliance over a quarter |
| 2 | Project Planning | Where additional deliverables are requested via a statement of work, the supplier will provide a detailed delivery plan within 5 working days | 95% compliance over a quarter |
| 3 | Project Reporting | Supplier operatives provide input to regular MyCO Programme reporting to monitor progress of the project as a whole.  Measured by completion and or input to Workstream lead monthly highlight report and Monthly contract deliverables progress review meetings. | 85% compliance over a quarter |
| 4 | Deliverable Tracking | Supplier operatives to regularly review and update MyCO Programme deliverables with Authority representatives.  Measured by creation and regularly maintained deliverable record. | 85% compliance over a quarter |
| 5 | Timeliness | Deliverables successfully delivered on time as per agreed plan | 85% |
| 6 | Customer Satisfaction | Departmental SMEs and MyCO Programme satisfaction with successful completion of deliverables.  Measured through DCA/SME delivery sign off. | 85% Very Satisfied |

# SECURITY AND CONFIDENTIALITY REQUIREMENTS

## All operatives will need to hold SC level government security clearance due to the sensitivity of some of the data sets and business transactions they will be privy to.

## The content of this Statement of Requirements is regarded as confidential and privileged and as such the Supplier should not disclose outside of their organisation.

# PAYMENT AND INVOICING

## Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

## Invoices will be raised on a monthly basis for progress against deliverables as agreed and signed off during monthly progress review meetings held between the Supplier, Programme Manager and Workstream leads.

## Before payment can be considered, each monthly invoice must include a detailed elemental breakdown of work completed and the associated costs against pre-agreed deliverable sets.

## Invoices should be submitted to: apinvoices-cab-u@gov.sscl.com and MyCO PMO Email mycoprogramme@cabinetoffice.gov.uk

## Monthly invoices raised by the supplier should clearly display the Cabinet Office Purchase Order Number.

# CONTRACT MANAGEMENT

## Contract progress review meetings will be held monthly with the Programme Manager and Workstream leads, for review of progress and authorisation to raise monthly invoices for payment against those set deliverables. There will also be weekly update meetings with Workstream leads which will feed performance updates to the Programme Director for MyCO Monthly highlight report meetings for which the supplier representative on occasion may be expected to attend.

## Attendance (whether in person or virtual) at Contract Review, Highlight report and weekly Workstream meetings with the Programme Director and SLT shall be at the Supplier’s own expense.

# LOCATION

## The location of the services will be carried out at 1 Horse Guards Road, 70 Whitehall, 10 South Colonnade and through remote working.