Crown Commercial Service

G-Cloud 13 Call-Off Contract

This Call-Off Contract for the G-Cloud 13 Framework Agreement (RM1557.13) includes:

G-Cloud 13 Call-Off Contract

Part A: Order Form

Buyers must use this template order form as the basis for all Call-Off Contracts and must refrain from accepting a Supplier's prepopulated version unless it has been carefully checked against template drafting.

Platform service ID number	174700475124464
Call-Off Contract reference	C235344
Call-Off Contract title	Business Continuity Management Software
Call-Off Contract description	Cloud-hosted business continuity management Software as a Service (SaaS) licences, support & maintenance.
Start date	30/03/2024
Expiry date	30/03/2026
Call-Off Contract value	£48,000
Charging method	Electronic invoice annually in advance.
Purchase order number	TBC

This Order Form is issued under the G-Cloud 13 Framework Agreement (RM1557.13).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Services offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

From the Buyer	NHS Business Services Authority Stella House Goldcrest Way Newburn Riverside Newcastle upon Tyne NE15 8NX
To the Supplier	[redacted] Company number: [redacted]
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: [redacted]
Name: [redacted]
Email: [redacted]

For the Supplier:

Title: [redacted]
Name: [redacted]
Phone: [redacted]
Email: [redacted]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 30/03/2024 and is valid for **24 Months,** with the option to extend by a further period of 12 months.
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least **90** Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	This Call-Off Contract can be extended by the Buyer for **one** period of up to 12 months, by giving the Supplier **4 weeks** written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below. Extensions which extend the Term beyond 36 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8. If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance: https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service

Buyer contractual details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

G-Cloud Lot	This Call-Off Contract is for the provision of Services Under: ● Lot 2: Cloud software
G-Cloud Services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below: -Licences for Business Continuity, Resilience and Risk Management Software -Hosting (SaaS) -Support
Additional Services	Not applicable.
Location	The Services will be delivered to the Buyer remotely unless otherwise agreed between Parties that Service will be delivered on-site at the following location: Stella House Goldcrest Way Newburn Riverside Newcastle upon Tyne NE15 8NX
Quality Standards	The quality standards required for this Call-Off Contract are as per service ID number 174700475124464
Technical Standards:	The technical standards used as a requirement for this Call-Off Contract are as per service ID number 174700475124464
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are set out in Schedule 1 and as per service ID number 174700475124464

Onboarding	Not applicable.
Offboarding	The offboarding plan for this Call-Off Contract is as follows: SQL backup is provided to the Buyer when contract ends. This contains all Buyer Data. The Buyer shall also have the facility to download all plans and documents stored within the BCMS in PDF, Word or other formats. The Buyer shall be entitled (but not obliged) to continue to use the Software and have access to all The Buyer generated data until it has another solution in place, such period not to exceed six months and provided that The Buyer pays a licence fee for any such period which is on a pro-rata
Collaboration agreement	Not applicable.
Limit on Parties' liability	Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed £100,000 per year. The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation, or damage to any Buyer Data will not exceed £100,000 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). The annual total liability of the Supplier for all other Defaults will not exceed the greater of **£100,000** or 125**%** of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).
Insurance	The Supplier insurance(s) required will be: • 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 the G-Cloud 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
Buyer's responsibilities	The Buyer is responsible for:

	• Appointing a day to day contact who will work as a conduit between Service Delivery Team during set up and indeed the duration of the partnership • Ensuring all those who will access the business continuity software have set up computers Laptops/ devices.
Buyer's equipment	Not applicable

Supplier's information

Subcontractors or partners	Sub-processors: Microsoft Azure and Twilio/Sendgrid https://www.twilio.com/trust https://www.microsoft.com/en-gb/trust-center

Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

Payment method	The payment method for this Call-Off Contract is BACS.
Payment profile	The payment profile for this Call-Off Contract is annual payment in advance. (£24,000 ex. VAT per year.)
Invoice details	The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.

Who and where to send invoices to	Invoices will be sent to NHS Business Services Authority, Stella House, Goldcrest Way, Newburn Riverside, Newcastle upon Tyne, NE15 8NX Email: accountspayable@nhsbsa.nhs.uk
Invoice information required	All invoices must include the call-Off Contract Reference and allocated Purchase Order Number
Invoice frequency	Invoice will be sent to the Buyer annually in advance.
Call-Off Contract value	The total value of this Call-Off Contract is £48,000 ex. VAT
Call-Off Contract charges	The breakdown of the Charges is detailed in Schedule 2 – Call-Off Contract Charges.

Additional Buyer terms

Performance of the Service	This Call-Off Contract will include the Services as set out in Schedule 1.

Guarantee	Not applicable
Warranties, representations	Not applicable
Supplemental requirements in addition to the Call-Off terms	Within the scope of the call-Off Contract, Part B: Terms and conditions 16. Security clause 16.1 shall be amended to provide that the Supplier must: Include within the Security Management Plan the reporting process for third party incidents to support the Supplier requiring reporting breaches of confidentiality.
Alternative clauses	Not applicable
Buyer specific amendments to/refinements of the Call-Off Contract terms	Within the scope of the Call-Off Contract, Part B: Terms and conditions 13. Buyer Data clause 13.6 will be amended to include the following: the National Cyber Security Centre's (NCSC) offline backups guidance: Offline backups in an online world - NCSC.GOV.UK the National Cyber Security Centre's (NCSC) guidance on secure system administration: Secure system administration - NCSC.GOV.UK
Personal Data and Data Subjects	Confirm whether Annex 1 (and Annex 2, if applicable) of Schedule 7 is being used: Annex 1
Intellectual Property	Not applicable.

Social Value	Fighting climate change - As per details provided with in service ID: 174700475124464

1. Formation of contract

1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.

1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.

1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.

1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.13.

Signed	On behalf of Supplier	On behalf of Buyer
Name	[redacted]	
Title	[redacted]	
Signature	[redacted]	
Date	[redacted]	

2.2 The Buyer provided an Order Form for Services to the Supplier.

Customer Benefits

For each Call-Off Contract please complete a customer benefits record, by following this link:

G-Cloud 13 Customer Benefit Record

Part B: Terms and conditions

1. Call-Off Contract Start date and length

1.1 The Supplier must start providing the Services on the date specified in the Order Form.

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 36 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 24 months.

2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 10 (Force majeure)
- 5.3 (Continuing rights)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)
- 17 (Bribery and corruption)
- 18 (Freedom of Information Act)
- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)
- 24 (Conflicts of interest and ethical walls)
- 25 (Publicity and branding)
- 26 (Equality and diversity)
- 28 (Data protection)
- 31 (Severability)
- 32 and 33 (Managing disputes and Mediation)
- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)

- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

2.2.1 a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'

2.2.2 a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'

2.2.3 a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 7 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'XX', where 'XX' is the Framework Agreement clause number.

2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

3. Supply of services

3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.

3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

4. Supplier staff

4.1 The Supplier Staff must:

4.1.1 be appropriately experienced, qualified and trained to supply the Services

4.1.2 apply all due skill, care and diligence in faithfully performing those duties

4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer

4.1.4 respond to any enquiries about the Services as soon as reasonably possible

4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer

4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.

4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.

4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.

4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.

4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

5.1 Both Parties agree that when entering into a Call-Off Contract they:

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

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

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

5.1.4 have entered into the Call-Off Contract relying on their own due diligence

6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their Service Descriptions.

6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.

7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoices under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

8. Recovery of sums due and right of set-off

8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

9. Insurance

9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

9.2 The Supplier will ensure that:

9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000

9.2.2 the third-party public and products liability insurance contains an ‘indemnity to principals’ clause for the Buyer’s benefit

9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

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

9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers

9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances

9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.

9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.

9.8 The Supplier will be liable for the payment of any:

9.8.1 premiums, which it will pay promptly
9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

10.1 The Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under incorporated Framework Agreement clause
34. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

11.1 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.

11.2 Neither Party shall have any right to use any of the other Party's names, logos or trade marks on any of its products or services without the other Party's prior written consent.

11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:

11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and

11.3.2 the Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer's written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.

11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

11.5 Subject to the limitation in Clause 24.3, the Buyer shall:

11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:
(a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
(b) alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;
(c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and

11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgment against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer's obligations under this Clause 11.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier's breach of this Contract.

11.6 The Supplier will, on written demand, fully indemnify the Buyer for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:

11.6.1 rights granted to the Buyer under this Call-Off Contract

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

11.7 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

11.7.1 modify the relevant part of the Services without reducing its functionality or performance

11.7.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer

11.7.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.8 Clause 11.6 will not apply if the IPR Claim is from:

11.8.1 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract

11.8.2 other material provided by the Buyer necessary for the Services

11.9 If the Supplier does not comply with this clause 11, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

12.1.1 comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data

12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body

12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

12.2.1 providing the Buyer with full details of the complaint or request

12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions

12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)

12.2.4 providing the Buyer with any information requested by the Data Subject

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

13. Buyer data

13.1 The Supplier must not remove any proprietary notices in the Buyer Data.

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

13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.

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

13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

13.6.1 the principles in the Security Policy Framework: https://www.gov.uk/government/publications/security-policy-framework and the Government Security - Classification policy: https:/www.gov.uk/government/publications/government-security-classifications

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: https://www.npsa.gov.uk/content/adopt-risk-management-approach and Protection of Sensitive Information and Assets: https://www.npsa.gov.uk/sensitive-information-assets

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance: https://www.ncsc.gov.uk/collection/risk-management-collection

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

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

13.6.6 Buyer requirements in respect of AI ethical standards.

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

13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

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

13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at: https://www.gov.uk/government/publications/technologycode-of-practice/technology -code-of-practice

14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.

15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

16. Security

16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.

16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.

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

16.4 Responsibility for costs will be at the:

16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided

16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control

16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.

16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:
https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

17. Guarantee

17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:

17.1.1 an executed Guarantee in the form at Schedule 5

17.1.2 a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided

18.2.2 Call-Off Contract Charges paid during the notice period are reasonable compensation and cover all the Supplier's avoidable costs or Losses

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied

18.4.2 any fraud

18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so

18.5.2 an Insolvency Event of the other Party happens

18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

19.4.1 any rights, remedies or obligations accrued before its Ending or expiration

19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry

19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)

- 24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability),
  24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

19.4.4 any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires.

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it

19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer

19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer

19.5.4 destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law

19.5.5 work with the Buyer on any ongoing work

19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

20. Notices

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

- Manner of delivery: email
- Deemed time of delivery: 9am on the first Working Day after sending
- Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message

20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the period on terms that are commercially reasonable and acceptable to the Buyer

21.6.2 there will be no adverse impact on service continuity

21.6.3 there is no vendor lock-in to the Supplier's Service at exit

21.6.4 it enables the Buyer to meet its obligations under the Technology Code of Practice

21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.

21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:

21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier

21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer

21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier

21.8.4 the testing and assurance strategy for exported Buyer Data

21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations

21.8.6 any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

22. Handover to replacement supplier

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control

22.1.2 other information reasonably requested by the Buyer

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than 30 consecutive days, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Supplier's liability:

24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited; and

24.2.2 in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.

24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).

24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause 24.2 will not be taken into consideration.

25. Premises

25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer's premises, the Supplier will:

25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises

25.5.2 comply with Buyer requirements for the conduct of personnel

25.5.3 comply with any health and safety measures implemented by the Buyer

25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

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

26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

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

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

27. The Contracts (Rights of Third Parties) Act 1999

27.1 Except as specified in clause 29.8, a person who isn't Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

28. Environmental requirements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

29.2.1 the activities they perform
29.2.2 age
29.2.3 start date

29.2.4 place of work
29.2.5 notice period
29.2.6 redundancy payment entitlement
29.2.7 salary, benefits and pension entitlements
29.2.8 employment status
29.2.9 identity of employer
29.2.10 working arrangements
29.2.11 outstanding liabilities
29.2.12 sickness absence
29.2.13 copies of all relevant employment contracts and related documents
29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

29.3 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

29.4 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.

29.4.1 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:

29.4.2 its failure to comply with the provisions of this clause

29.4.3 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

29.5 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

29.6 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.

31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:

31.2.1 work proactively and in good faith with each of the Buyer's contractors

31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

32.1 The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.

32.3 If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days notice to the Supplier.

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7.

Schedule 1: Services

Continuity2's Meridian BCMS

Business Continuity, Resilience and Risk Management

Software with Hosting (SaaS)

Service Definition Document

Contents

Overview of Meridian BCMS

The Meridian BCMS software is a secure web-based tool designed to alleviate and assist with the day to day management of an Organisation's BCMS.

The tooling is consistent with many, if not all, of the requirements of good practice in Business Continuity Management ISO 22301. The tool is an integrated BC Quality Management System:

Meridian BCMS allows you to create, store, manage and distribute business continuity Plans. The scheduling and carrying out of Exercises is simple with results reported via the system. In the event of an incident you can contact key personnel or groups of staff via 2-way SMS, voice calls, email and conference calling with real time reporting and tracking. Continuity2 is committed to promoting best practice in Business Continuity Management and supporting this through its Business Continuity Software.

Meridian BCMS delivers:

- Creating and managing business continuity plans
- Conducting business impact analysis
- Conducting Important Business Services Analysis (IBS)
- Exercising of business continuity plans
- Policy or key performance indicators control
- Contacting / notification of personnel during incidents and exercises
- Maintaining and accessing vital records
- The provision of audit capability
- BC Risk Management
- MI and reporting
- The creation and tracking of corrective/ preventive actions
- Mobile notificationn and Plan Functionality

Plan Management

Plans can be created automatically by this system via a combination of the dynamic template capability (the ability to build templates and have them automatically read data from e.g.
BIA, contact lists, systems lists, supplier lists etc.) Plans are automatically version controlled, reviewed, and distributed and signed off according to your change control procedures by the workflow. Contact details are held in a central database for use in plans and call lists. Updates to contact details are applied

and available immediately. Plan managers / coordinators have an intuitive dashboard to manage their plans from. We recognize that the plan, alone, may not be enough documentation in the even to of a BC incident. So, we provide an "Associated Documents" ('Virtual Battle box') facility to store associated documentation for each plan which may be used in the event of an incident. Changes to all plans across the enterprise can be performed simultaneously via the central administration.

Efficiencies / Benefits

Plans can be of any type (e.g. emergency procedures, business continuity plans, IT disaster recovery plans and crisis management plans). During implementation, we will train your administrator/s on the use of the proprietary Continuity2 **Template Creator** and assist them with the creation of the initial templates to suit your organization. Template changes are reflected across all documents associated to that template e.g. if a template has been used across 100s or 1000s of plans then any change to the template is reflected automatically across all the documents. Templates can be aligned to recognsied BCM best practice e.g. Business Continuity Institute's Good Practice Guidelines, Disaster Recovery Institute, ITIL and ISO 22301.
Business Impact analysis data is automatically input into plans. Indeed, in many cases the automated workflow can eliminate the need to develop BC plans in that the combination of the centrally driven template and integration to BIA information provides 100% of plan content. For BIA see below:

Business Impact Analysis

The Business Impact Analysis module is intuitive and follows best practice and International Standard e.g. ISO27001 requirements: BIA's are integrated into the system and can be carried out at all points of the enterprise e.g. Organisational, Directorate / Business Unit and / or Service / Functional levels.

The BIA identifies Key Products and Services and their supporting activities. The activities are analysed under the organization's criteria for impact analysis i.e. the system is configurable via the BIA administration function within the system to reflect the organisation's criteria for analysis.
Critical activities are identified together with their supporting resources, dependencies and recovery requirements. This data is automatically made available to plans thereby providing the basis for plan content. Consolidated BIA data is produced in the form of PDF / word reports which can be automatically sent for review and sign off. BIA/Risk Analysis is integrated completely within the software.

Efficiencies / Benefits

The BIA is facilitated via an online wizard where responders / participants answer questions regarding their activity / service. The data is captured with the system as required by the organisation, and thereafter is available for reporting and planning purposes. Responders require no training and are generally not users of the system. Their participation is facilitated via email linking them to their specific analysis which takes on average 30 minutes to complete on the 1st pass of the BIA and 10 – 15 minutes to review thereafter (normally annually). The combined participation of the responders provides core planning data without the need for workshops / interviews and extensive proforma exercises.

Important Business Services Analysis (IBS)

IBS Management allows the System Administrator to create and manage Import Business Services (IBS) from a single central interface. IBSIA Management also acts as a tool to assign ownership of services and the distribution of Important Business Service Impact Analysis.
The IBS Impact analysis can either be run directly from IBSIA Management by the logged in System Administrator, distributed via email to be conducted by a service plan owner from within the IBS Plan Management module (should you decide to create IBS Continuity Plans).

When distributed the IBS Impact Analysis is accessed by the service owner via an email link. The service owner will then be presented with a dedicated landing page full of helpful information that will guide them through the analysis itself. As a System Administrator you will be able to control the control which is presented to the service owner on this landing page via the IBSIA Administration. IBSIA Administration also allows you to completely configure the IBSIA to your organisations requirements for analysis.

With a vast array of elements to keep track of across your service continuity programme it is critical you have a central location that can provide a clear view of your current performance. The IBS MI Performance Dashboard provides you with an overarching view of your programme. Once you have found the information you are looking for then pull off a summary report at the click of a button

Plan Exercise Management

We recognise that the exerting of plans is essential to the overall assurance process that we are capable of mitigating business interruption impact. We also recognise that it would be great if the system would arrange these exercises i.e. set the frequency, type, objectives, invite participants and link to our incident management /plan notification module. So, we developed the workflow that allows you as the organisation to set the importance of plans according to the impact they are mitigating. This can either be referred to as **policy or key performance indicators. E**ither way, the Exercising module creates the exercise types per the organisation's preference and the policy which the plan is subject to, schedules the exercise (as per the policy), invites the participants, defines the exercise objectives and emails the details to the participants. On completion of the exercise the system reports on the observations of the exercise and tracks recommendations and actions raised as a result of the exercise. All exercise reports can be distributed and signed off via the system and held within the system for Audit purposes.

Efficiencies / Benefits

The capability of the system to automatically create the exercise schedules, at your appetite, results in a massive time saving on: Organizing exercising schedules, communicating where when what, training of plan mangers on how to organize their exercises i.e. there is **no effort** on these tasks as the system automatically does them.

Policy or key performance indicators control

As discussed in the exercise management section, we have developed the workflow engine that allows you as the organisation to set the importance of plans according to the impact they are mitigating. This is a fantastic time / user training saving i.e. as an administrator you can decide what the frequency of BIA, Plan, Exercise, Training reviews are, and the system will automatically manage all of this for you and report the progress to the management information dashboard.

Management Information

Meridian BCMS includes a fully functional Management Information module that reports on e.g. the currency of BIAs, Plans, Exercises and Communication. The system produces graphical views of performance and downloadable management reports. This function allows organizations to set metrics for performance of their BCMS and measure progress against BCMS objectives.
Reports can be produced at any level within the organisation e.g. Organisational, Regional, Country, Business Unit, Business Function etc.

Efficiencies / Benefits

The system requires no user effort to compile the management information other than clicking the MI button to view the graphical data and download the reports. This interface is often the focal point of steering group meetings and discussion as it provides a real-time view of the health of the management system without the need for extensive pre-meeting preparation. You can view performance at any level of the system provides reports in PDF and Word to support all MI. Report can be sent to stakeholders automatically at the desired frequency.

Plan Incident and Notification Management

The system has a fully functional Notification / Incident Management capability including **two-way SMS, Voice Messaging**, **Action Creation / Tracking**, and **Call Conferencing.** The Incident Management system enables the team controlling the incident to call out and stay in touch with people during incidents. The system allows the communication with individuals, recovery teams and others in the enterprise as needed. The technology built into the system allows for the setting up of web-based incident pages and task lists where stakeholders can be kept up to date on incident status via push or pull messages through email including mobile devices.

The system also has a mobile interface that works on any browser compatible smart phone e.g. Android, iPhone, and Blackberry. The mobile interface allows users to view plans, view associated documents, view check lists, communicate with team members, conduct conference calls, send SMS and send Text to Voice messages.

Efficiencies / Benefits

The integral communication capabilities and data interfaces within the system allow for efficient collation of contact data and execution of communications during incidents. The updating of contact details and keeping call lists up to date can be time consuming; the system provides the ability for call lists to be maintained with a minimum level of effort to the extent that the system will build and maintain call lists automatically as a result of data import or SFTP automation. Whatever method is chosen by an organisation; the system negates the need for administrators to build and maintain call lists.

Additional Call lists

Essentially this gives our clients the ability to create notification lists for anything within their organisation. Unlike plan incident notification, there does not need to be a plan present i.e. you can create notifications for any locations, functions, departments, groups of people, specific project etc. etc.

Risk Management

The C2 RM module allows you to design your own approach to BC risk and maintain risk assessments and risk registers throughout the organisation. This module is and will continually be developed to provide users with the ability to control Resilience Risk across the organisation.

Corrective Action Tracking

Meridian BCMS includes a fully functional corrective action tracking system which can be used to track all corrective actions associated to the management system e.g. actions from audits, exercises, BIA, etc.

Efficiencies / Benefits

If desired the system enables the raising, reporting and tracking of all corrective actions automatically sending and receiving of updates on status and requests for closure. It is fully compliant with ISO requirements for corrective action.

Internal auditing

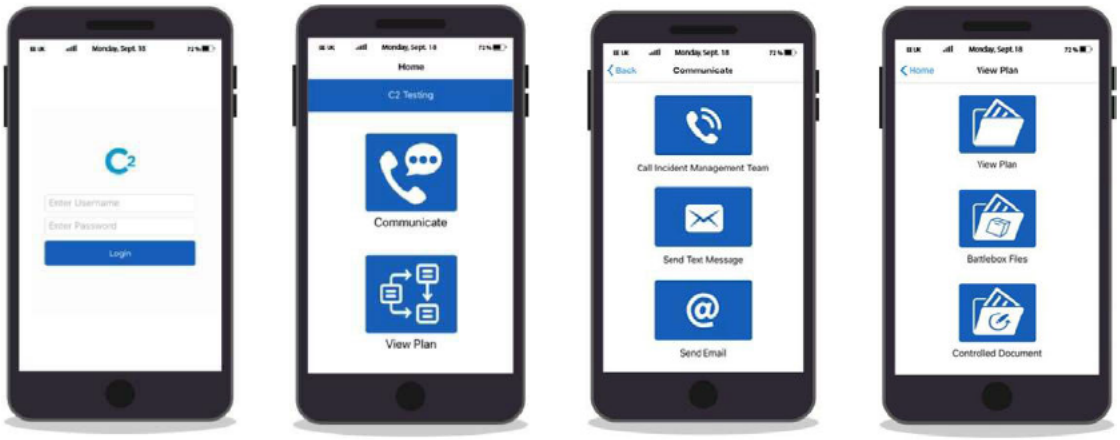
Internal auditing of the organisation's BCMS can be conducted via the setting of audit questions and the delivery of questions to participants in the audit via an online interface. The interface allows participants to respond to the audit and provide evidence to support their responses to the audit. The system provides an effective method of conducting audits with minimal effort and is compliant to quality management systems requirements e.g. ISO 22301 ISO 27001:

Surveys can be executed and reported on via the system to provide assurance to management of e.g. BC capabilities, Supply Chain Analysis, Requirements Reviews etc.

Efficiencies / Benefits

The system provides ability to audit the BCMS with minimal effort i.e. instead of utilising a rolling audit programme (2, 3 years) with the subsequent interviews and meetings. Audits can be carried out within a 2 / 3 week lapsed time with 3 / 4 days efforts. Audits are saved and can be reused / edited for future use thus saving on preparation time.

Mobile Functionality



Meridian BCMS allows true seamless high availability of BC plans through your own mobile technology. Our app synchronizes with your live data enabling you or indeed any member of your incident management team to view plans and strategies, call trees, battlebox and other associated documents whilst on the move. The mobile application negates the old requirements for "hard copy" BCPs, enhancing information security protocols by ensuring that everyone has access to the right information, right when they need it. The mobile app adds another layer of protection by ensuring that, should your Meridian BCMS tool be offline, your critical information is still available.

Efficiencies / Benefits

Speed of response is critical in an incident. By providing immediate access to your plans, call tree information and crisis communication mechanisms, you are minimising potentially negative impacts on your brand and reputation by projecting a confident public image as a result of a collaborative, coordinated and, importantly, swift response. The app (available for iPhone or Android) provides the ability to view plans, battle box files or essential controlled documents (plans, maps etc.) as well as initiating your crisis or incident response via SMS or email. A key feature is the ability to undertake a "recovery team" pull conference call, without the need for dial in numbers, pins or passwords.

Reports

The application comes with the ability to run dynamic reports than can be used to inform management either in the daily management of business continuity or incidents e.g.:

- Tell me what processes are affected by the loss of this system,
- Tell me what services / process are affected by the loss of this site,
- Tell me what resources are required to recover this process
- Tell me the number of staff that can work from home in this location
- Tell me the number of staff that require alternative working arrangements
- Tell me the number of phones, PCs, Desks, Laptop required
- Tell me the application required over time required to support this specific incident
- Etc. etc.

Reports are in PDF and or Excel formats.

Efficiencies / Benefits

In that BIA data is collated and maintained efficiently it can be scrutinised to provide dynamic reports as detailed above. This eliminates the need to scrutinise documentation (e.g. reports and spreadsheets) manually and extrapolate information on a manual basis.

Document Management System

In Addition to Plan document control, the system provides a full document management system for all BCMS documentation under change control e.g. Policy, Methodologies, Reports, Minutes to meetings, Training Records etc.
The Document control function allows users to set the parameters for **reminder emails** to be sent for the review and sign-off of documents, as well as being able to monitor at what stage a document is in within the review / sign off process. Document control displays the review and sign off status of Plans, BIAs, Exercises and BCMS documents within the application and can be viewed by document type as well as document type within Business unit.

Efficiencies / Benefits

The system provides an efficient workflow that traces all documentation and maintains the currency of documentation via the Web-service. Once documents are uploaded and

assigned to the system there is no requirement for user intervention. Interventions are only required when the workflow for a document is interrupted e.g. an author leaves the organisation, a signoff date is missed. This is flagged to the administration who can reallocate the authorship to another contact with ease.

Resilience, Backup and Restore

Microsoft Azure provides the foundation on which the system is built. This has been configured in accordance with the Azure Security Benchmark (ASB) that provides prescriptive best practices and recommendations that help improve the security of workloads, data, and services on Azure.

Based on Kubernetes (AKS) and container technologies, the service platform is deployed in a highly available configuration within Azure Regions ensuring no single point of failure. Each AKS cluster is distributed across multiple availability zones (data centres within a region) to ensure that even if a data centre were to be lost, the system will be automatically recovered to a different availability zone within the same region. All data (DB and file storage) is replicated in real-time across these same availability zones to ensure that no matter where the system is running or if a data centre is lost, your data will always be available and up to date.

As well as this, data backups are geo-replicated to a separate, nearby Azure Region to ensure that in the highly unlikely case that an entire Region is lost (multiple data centres), the services can be resumed from another.

A virtual private network with all communications carried out using TLS1.2.

Firewalls control all access to the infrastructure and provide protection against attacks such as DDoS. Web Application Firewall (WAF) is configured based on rules from the OWASP (Open Web Application Security Project) core rule sets.

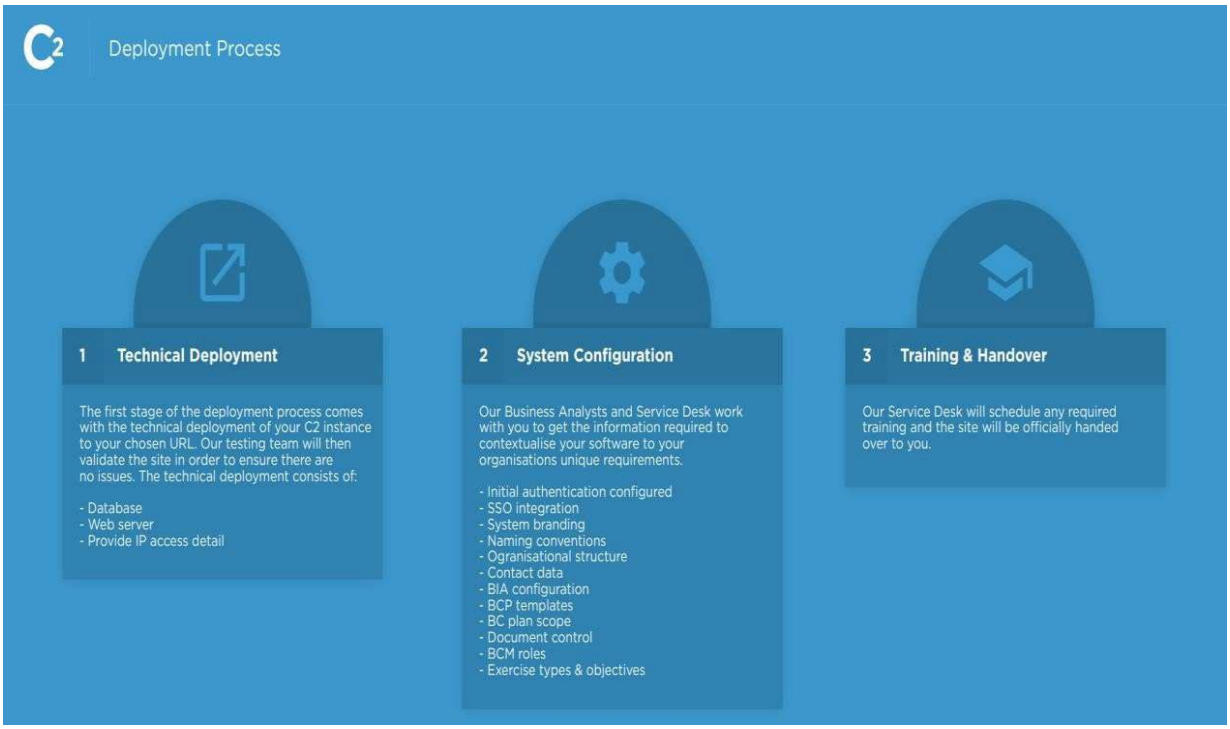
Each customer has their own dedicated compute, database, and file storage facility ensuring isolation from others.

On Boarding and Off Boarding Support

Onboarding

On deployment of MBCMS, C2 will provide a full user guide on the application along with quick reference guides, these will be digital copies so they can be stored and used on-the-go. A project plan is agreed and shared with the customer upon contract award. Should the Customer be moving from another solution, we will engage with The Customer to try and make the switch to our platform as smooth as possible and prevent duplication of any work.

Following the MBCMS deployment we offer additional training sessions for admins which can either be carried out via online web-sessions or we can arrange further onsite training. C2 adopt the "Train the trainer" approach so we endeavor to ensure that your system admins are in a position to provide further training to any potential new users during their internal roll-out of the system.



Offboarding

C2 will fully support the customer with an exit plan.

SQL backup is provided to the Buyer when contract ends. This contains all Buyer Data. The Buyer shall also have the facility to download all plans and documents stored within the BCMS in PDF, Word or other formats.

The Buyer shall be entitled (but not obliged) to continue to use the Software and have access to all The Buyer generated data until it has another solution in place, such period not to exceed six months and provided that The Buyer pays a licence fee for any such period which is on a pro-rata.

After the contract ends Continuity2 is obliged to deliver within one month after the effective date of the termination to The Customer all Customer data stored in the Software in an electronic form to be agreed between the parties.

Maintenance and Customization

Each customer environment is encapsulated within a Docker container environment. These environments are ephemeral and therefore are not patched but instead will be redeployed using automated blue/green deployment processes when updates are provided from platform suppliers such as Microsoft for Windows OS or as a result of a security vulnerability / update.

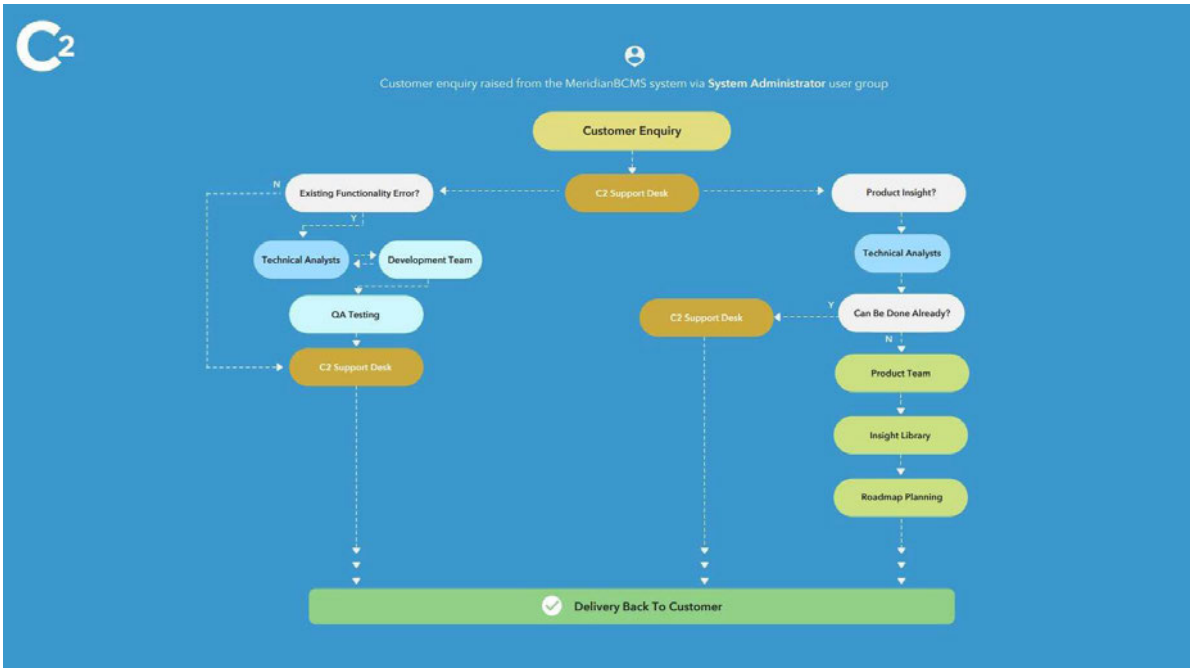
As well as this, data backups are geo-replicated to a separate, nearby Azure Region to ensure that in the highly unlikely case that an entire Region is lost (multiple data centres), the services can be resumed from another.

Vulnerability scans are carried out continuously on both production and development environments as well as penetration testing being carried out by a CREST certified 3rd party on an at least an annual basis.

All client change requests fall under C2's change management policy. Requests are collated and reviewed internally by our Design Authority. If requests are approved then these would be updated onto the release schedule once timescales have been determined.

Clients are not allocated specific customization allowances but are entitled to raise requests for change which are put forward for review.

Service Availability & Support



The availability of the system is monitored 24x7x365 and system restoration due to major fault is managed to return to operation within the SLA target.

For general "how to" enquiries Continuity² provide a personal help desk between the hours of 08.00 and 18.00 UK Standard Time, Monday through Friday, with the exception of Christmas Day, Boxing Day, New Year's Day and the first working day of January.

Continuity² shall have no obligation to provide the services outside its normal business hours.

Users can report issues from either within the application, via the Issue button or by telephone (08450944420), the details of the fault / issue are be logged on our Incident management systems and these are passed directly to Continuity2 support. If the user logs the fault via the application, they will receive an email confirmation of their fault number and a summary of the fault that they logged.

For the Continuity2 System / Application there are 3 levels of support available: -

First support level - all faults / queries should be directed to The Customer 's System Administrator, who will be able to answer most "How do I?" questions. Should the system administrator be unable to resolve the fault / issue, they will then log it with second level support, the Continuity2 helpdesk or Ticketing facility

Second support level - Continuity2 helpdesk who will answer technical questions and log faults for The Customer Systems Administrator, in all instances contact will be made with the user within 2hours of a query being raised, and confirmation of actions being taken passed to the user.

Third support level - Continuity2 development team who will be passed those faults / issues not resolved by the first two levels of support, faults will only be accepted by third level support via the on line ticketing system. Contact will be made with the Customer System's Administrator within 4 hours of the fault being passed to third level support.

The Customer's Systems Administrator will be updated on the incident regularly and can phone helpdesk at any time for updates. The incident is closed when the user is satisfied that it is resolved.

Incidents are logged and prioritised within the Service Desk. These are then monitored to ensure that they are being actioned and progressed to completion. If an incident is going to miss its resolution time then the client is informed and it is escalated within the Service desk and to senior management to ensure that the correct resources are deployed to assist in resolution. Clients are provided with updates via the issue ticket and by telephone if requested, at agreed time periods until the issue is resolved.

Priority response and fix

Continuity² shall respond to The Customer request for assistance in line with the table below of The Customer entering the request in the on-line ticketing facility.

Priority	Description	Initial Response	Resolution to Fault within
P1	Use of the System / Application is not possible and no work around is available. *Technical issues where the fault is within the infrastructure / continuity² network environment i.e. user cannot access the system.* *24x7x365 service provision*	30 minutes	3 hours
P2	A substantially System / Application can still be used but a feature is not available. *Technical code level issues where the fault is within a module e.g. BIA,* *24x7x365 service provision*	2 hours	48 hours
P3	Loss of some operational functionality in the System / Application but a substantially the System / Application can be used without an adverse impact. Core functions are operating e.g. Notification, fault is within a feature not the feature itself. *Support related issues were the helpdesk manage resolution e.g. cannot access / use calendar functions to organise exercises, audits, training in advance.* *Response and Resolution timings to fault can be triggered between 08:00 and 18:00 GMT*	3 hours	4 days
P4	Minor fault affecting operational functionality e.g. link between the data and a plan needs formatting / re- establishing. *Support related issues where the helpdesk manage resolution e.g. cannot capture some specific BIA information with a field but can capture elsewhere within the system in the interim.* *Response and Resolution timings to fault can be triggered between 08:00 and 18:00 GMT*	4 hours	8 days

P5	Minor fault not affecting operational functionality e.g. cosmetic UI, formatting within a report. *Support related issues where the helpdesk manage resolution e.g. system colours, layout, hard code wording etc.* *Response and Resolution timings to fault can be triggered between 08:00 and 18:00 GMT*	8 hours	16 days

Technical Requirements

Minimum and recommended specifications for user workstations

Hardware:

- PC / Laptop / Mac
- Recommended 4GB Ram, I3 processor or above
- 10Mb Download speed recommended

Software:

- Browser Software (Chrome, Edge & Safari)
- Microsoft Office 2007 minimum

Statement of Requirements
C235344 Business Continuity Management Software

Requirements		
Id No.	**Description**	**Priority** ***M = Must Have*** ***S = Should Have*** ***C = Could Have***
1.0	**BCM Software Execution and Delivery**	
1.1	The solution must have the capability to be structured to align to the customer's services and current policies and procedures	M
1.2	The solution should have the ability to reflect both internal and external issues	S
1.3	The solution should have the ability to report on overall RAG status and sub-RAG statuses	S
1.4	The solution should have the ability to link risks and issues to defined service areas	S
1.5	The solution must have the ability to link risks and issues with corrective actions	M
1.6	The solution should allow for high level performance tracking of BCM overall and at individual service level	S
1.7	The solution should have the ability to report on the overall health of the BCMS using RAG status	S
1.8	The solution should have the ability to maintain a cumulative view of BCM programme risks and issues	S
1.9	The solution should have the ability to report an executive summary on the state of the BCM programme	S
1.10	The Solution should be able to link/ roll up detail from project/programmes and corresponding business continuity plans	S
1.11	The solution should have the ability to maintain a cumulative view of BCM programme performance	S
1.12	The solution must have the ability to record service information e.g. location, activities, number of staff, owner	M
1.13	The solution must have the ability to be customizable by the buyer i.e. the reports produced and the layout of business continuity plans	M
1.14	The solution should have the ability to record an executive summary on the status of each business continuity plan i.e. Completed this month, planned activities for next month	S
1.15	The solution must have the ability to record and measure key metrics, for example, Recovery Time Objectives, Maximum Tolerable Period of Disruption	M
1.16	The solution must have the ability to capture key interested parties and stakeholders	M
1.17	The solution must have the ability to reflect the priority of service recovery	M
1.18	The solution must provide templates for the completion of BC documentation, including Business Impact Analysis (BIA) and Business Continuity Plans (BCP).	M
1.19	The solution must provide configuration to enable the Customer's administrator to make changes to the content and structure of BIAs and BCPs without the need to engage the supplier for development	M
1.20	The solution should have the ability to add updates/ notes against a service area's business continuity documentation	S
1.21	The solution must have the ability to import incident information from the BSA existing IT Service Management tool	M
1.22	The solution must have the ability to export information to the BSA existing IT Service Management tool	M
1.23	The solution should have the ability to record incidents and the impact to our services	S
1.24	The solution should have the ability to archive closed incidents	S

1.25	The solution should be capable of identifying incidents that are no longer active	S
1.26	The solution should allow users to search based on historical incidents, using time period as a parameter	S
1.27	The solution should have the ability to capture lessons learned from incidents	S
1.28	The solution should have an organization mapping tool to display roles, responsibilities and escalation pathways	S
1.29	The solution must allow for the definition of different role types, for example system admin, business continuity coordinator, business continuity manager	M
1.30	The solution must have an instant messaging functionality to allow for fast effective communication during an incident	M
1.31	The solution must allow for individual contact details to be added, edited and deleted without supplier intervention	M
1.32	The solution should allow users to edit and delete their personal information at any time	S
1.33	The solution should indicate the status of each business continuity document, i.e. draft or approved	S
1.34	The supplier should provide comprehensive training in use of the solution to defined individuals i.e. administrative users	S
1.35	The solution must have an EDRM (Electronic Document and Records Management) facility	M
2.0	**Reporting**	
2.1	The solution must be capable of generating summary reports of the performance of the BCM	M
2.2	The solution must have an approval system that accounts for review, update, approval and distribution of key documentation	M
2.3	The solution should be capable of producing reports applicable to varying audiences i.e. service lead – health of the BCMS, executive summary and Incident Reports	S
2.4	The solution must have the ability to add, edit, delete and baseline key business continuity criteria	M
2.5	The solution could have the ability to make template checkpoints for varying priority of service area	C
2.6	The solution should have the ability to upload existing information in email or document format, including Word/Excel/PDF/JPEG	S
2.7	The solution should have the ability to assign actions to identified individuals and service areas	S
3.0	**Risk & Issue Management**	
3.1	The solution must have the ability to log and manage Risks and Issues at strategic level, service area and activity level	M
3.2	The solution must have the ability to assign unique references to risks and issues at service area and activity level	M
3.3	The solution must be configurable to add/manage risks in accordance with the NHSBSA Risk Management Framework (Appendix 1), one of the key Customer policies.	M
3.4	The solution should have the ability to score risks and issues using a RAG rating	S
3.5	The solution must have the ability to capture and track mitigation / corrective actions	M
3.6	The solution must have the ability to capture mitigated impact and likelihood of risks	M
3.7	The solution must be capable of generating reports on identified risks and where there are mitigations in place	M
3.8	The solution must have the ability to assign an owner to risks and issues	M
3.9	The solution must allow for priority and deadline to be assigned to identified risks and issues	M

3.10	The solution must have the ability to add, update and delete risk and issue fields with BSA specific categorisation, drop downs and titles i.e. risk type, sub categories, root cause	M
3.11	The solution must have the ability to track dates against risks and issues e.g. created date, Review date, closed date	M
3.12	The solution must have the ability to export risks and issues into a suitable format such as excel / PDF, for presentation purposes	M
3.13	The solution should allow escalation of risks and issues to appropriate, identified individuals	S
3.14	The solution should enable the cross referencing of underlying service level risks to summarised organisational level risks	S
3.15	The solution should be able to identify where risks have not been reviewed	S
3.16	The solution should have the ability to add updates / notes against a risk or issues	S
3.17	The solution should have the ability to capture when a risk or issue is created/updated/deleted who carried out the action and when it was carried out	S
3.18	The solution should have the ability to notify the affected service areas of particular risks or threats	S
3.19	The solution should have the ability to archive risks	S
3.20	The solution should have the ability to assign risks to multiple affected areas	S
3.21	The solution must have the ability to transfer risks between service areas	M
3.22	The solution could have the ability to upload amendments to risks and issues via excel	C
4.0	**Administration / management**	
4.1	The solution must provide a documented manual and instructions i.e. user guide	M
4.2	The solution must have the ability to segregate/ restrict access rights for areas such as amending BC documentation, communicating documentation/ incident updates and generating MI reports	M
4.3	The solution must have the ability to create, edit and delete departments in the system	M
4.4	The solution should have the ability to create, edit and delete sub departments in the system	S
4.5	The solution must have the ability to create, edit and delete named resources in the system and link them to a department or sub department.	M
4.6	The solution should have the ability to add, edit, delete and show vacant resources in departments as well as single points of failure	S
4.7	The solution should have the ability to notify service areas of a gap in key BC resource i.e. link to leavers process	S
4.8	The solution should have the ability to set up and maintain a skills matrix against identified roles i.e. BC Coordinator	S
4.9	The solution should have the ability to notify identified individuals of any skills/training gaps	S
4.10	The solution should prompt service areas to identify delegates for each BC role	S
4.11	The Solution could have the ability to import annual leave via spread sheets	C
4.12	The Solution could have the ability to request resources via workflow to resource managers	C
4.13	The Solution could have the ability to notify a user when they are allocated to BC plans	C
5.0	**Usability**	
5.1	The solution should have a search function by keywords.	S
5.2	The solution must have customisable fields that admin can change without the need for supplier intervention.	M
5.3	The solution should show when a page is loading i.e. loading symbol	S

5.4	The solution could notify a user before the system times out to ensure work is not lost	C
5.5	The solution must have auto save capability	M
5.6	The solution could have the ability to apply customized help/guidance on fields i.e. pop up help when cursor hovers over a field	C
5.7	The solution should have a licensing arrangement to allow portal/dashboard access without incurring licensing charges.	S
6.0	**Overall solution**	
6.1	The solution must support the right to be forgotten by enabling deletion of staff records upon request.	M
6.2	The solution must not store or otherwise transfer personal data outside of the UK.	M
6.3	The solution must allow the BSA to enforce its data retention requirements and additional requirements detailed in Data Protection legislation including General Data Protection Regulation.	M
6.4	Access to different parts of the solution must be controlled by user groups, roles and permissions and managed by the admin users	M
6.5	Provide all necessary assistance and cooperation as reasonably requested by the NHSBSA to enable the NHSBSA to comply with its obligations under the FOIA at no additional charge	M
6.6	Data must be securely destroyed at the end of the contract or 30days by default unless agreed end of the retention period with NHSBSA. Secure destruction means physical storage media destruction or repeatedly re-writing over the media until the original information can no longer be retrieved. This must be achieved to the standard BS EN 15713:2009 or any standard that supersedes it	M
7.0	**Access Security**	
7.1	The solution should identify inactive accounts.	S
7.2	The solution should have the ability to segregate roles and views throughout the tool, for example, Full admin access, read only access	S
7.3	The solution must be able to restrict write access to certain business continuity documentation and identified sections of business continuity	M
7.4	The solution should have the ability to control access levels to information, for example through read-only or write access	S
7.5	The solution must have the ability to create an audit trail of any amendments made to documentation	M
8.0	**Collaboration/ Integration**	
8.1	The Solution could have a Document Repository to allow for sharing of content	C
8.2	The solution could allow collaborative working, promoting learning with forums and chat functions	C
8.3	The Solution could have the ability to integrate with MS Outlook for email and calendars	C
9.0	**Non-Functional Requirements**	
9.1	**Security and Governance**	
9.1.1	The Supplier shall ensure that the Services are compliant with the requirements and controls of ISO27001 as a minimum.	M
9.1.2	All passwords must be stored securely as detailed in Cabinet Office guidance Tip 7 and be implemented in line with the latest NCSC guidance (https://www.ncsc.gov.uk/guidance/password-collection).	M
9.1.3	The solution must provide a transparent audit trail of all user activities including create, update, delete, view and the download of data which can be reported on and interrogated by the Authority. All the Services shall have the ability to capture events at internal user, external user, supplier and system level and pass events to a syslog server.	M

	The available logs and audit functionality must be documented and accessible to an end internal user who has the ability to view audit information.	
9.2	**Reliability**	
9.2.1	The solution must have a mean recovery time period for business continuity planning functionality of a maximum of 48 hours between the service being detected in a down state to an available state form a user's perspective.	M
9.2.2	The solution must have a mean recovery time period for incident management functionality of a maximum of 12 hours between the service being detected in a down state to an available state form a user's perspective.	M
9.3	**Usability**	
9.3.1	The solution must be compatible with and supported for the following browsers: Safari, Internet Explorer 11, Edge, Chrome, Firefox.	M
9.3.2	The solution must be capable of supporting incident notifications to be alerted to end users via all mobile device types, including both iOS and Android.	M
9.3.4	The solution's screen resolution should match the current workstation resolutions for accessing current business continuity data.	S
9.3.5	The solution should be AA accessibility compliant, as defined by the W3C Web Content Accessibility Guidelines (WCAG) 2.1.	S
9.3.6	The solution should be compliant with assistive technologies in compliance with GDS standards https://www.gov.uk/service-manual/technology/testing-with-assistive-technologies.	S
9.3.7	The system must notify the user of any system errors.	M
9.3.8	The solution must have the ability for both internal and external third party users to have access to all functionality.	M
9.4	**Performance**	
9.4.1	The time taken for a user to log into the system's User Interface should not exceed 5 seconds from when correct logon credentials are entered.	S
9.4.2	The time taken for a user to load the system's User Interface pages should not exceed 5 seconds from the request.	S
9.4.3	The time taken for the system to notify an end user of an incident occurring should not exceed 5 seconds from the notification being sent.	S
9.4.4	The time taken to download an incident management report should not exceed 15 seconds.	S
9.4.5	The time taken to download a management information report should not exceed 20 seconds.	S
9.4.6	The time taken to load the business continuity plan pages should not exceed 10 seconds.	S
9.4.7	The time taken to load incident management pages should not exceed 5 seconds.	S
9.5	**Scalability**	
9.5.1	All geographical locations for system to be accessed from by different users, including over the internet and NHSBSA network (including homeworking)	M
9.5.2	The system must be scalable to support predicted business growth (as stated in the scope 100% within 4 years)	M
9.5.3	The solution must continue to meet the Performance Requirements when additional data is added to the system by the Customer.	M
9.6	**Capacity**	
9.6.1	The solution must allow the storage of data 4 years, to the end of the contract and allow access to the NHSBSA data beyond 4 years	M
9.6.2	The solution must provide storage space of up to 500GB or to support the initially stated scope and business growth	M
9.7	**Availability**	
9.7.1	The Supplier and Customer must agree all planned outages in advance.	M
9.7.2	The solution must have an uptime Availability of 99.5%.	M
9.8	**Interoperability**	

9.8.1	The solution must have the ability to pull incident management information from the Customer's incident management software.	M
9.8.2	The solution must have the ability to send business continuity information to the Customer's incident management software.	M
9.8.3	The solution must be capable of exporting Management Information report data to external systems in standard formats, including .csv and .xlsx.	M
9.9	**Integrity**	
9.9.1	For incident data downloads, the solution must be able to report when the data download has failed.	M

Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Platform pricing document) can't be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will include:

For the license for Meridian BCMS covering period 30th March 2024 – 30th March 2026 Annual license fee is inclusive of 2nd line support, hosting, maintenance and enduring 4 days consultative support **Please note this is billed annually at £24,000**	£48,000

Schedule 3: Collaboration agreement

Not Used.

Schedule 4: Alternative clauses

1. Introduction

1.1 This Schedule specifies the alternative clauses that may be requested in the Order Form and, if requested in the Order Form, will apply to this Call-Off Contract.

2. Clauses selected

2.1 The Customer may, in the Order Form, request the following alternative Clauses:

2.1.1 Scots Law and Jurisdiction

2.1.2 References to England and Wales in incorporated Framework Agreement clause 15.1 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.

2.1.3 Reference to England and Wales in Working Days definition within the Glossary and interpretations section will be replaced with Scotland.

2.1.4 References to the Contracts (Rights of Third Parties) Act 1999 will be removed in clause 27.1. Reference to the Freedom of Information Act 2000 within the defined terms for 'FoIA/Freedom of Information Act' to be replaced with Freedom of Information (Scotland) Act 2002.

2.1.5 Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.1.

2.1.6 References to "tort" will be replaced with "delict" throughout

2.2 The Customer may, in the Order Form, request the following Alternative Clauses:

2.2.1 Northern Ireland Law (see paragraph 2.3, 2.4, 2.5, 2.6 and 2.7 of this Schedule)

2.3 Discrimination

2.3.1 The Supplier will comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular the:

- Employment (Northern Ireland) Order 2002
- Fair Employment and Treatment (Northern Ireland) Order 1998
- Sex Discrimination (Northern Ireland) Order 1976 and 1988
- Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003
- Equal Pay Act (Northern Ireland) 1970
- Disability Discrimination Act 1995
- Race Relations (Northern Ireland) Order 1997
- Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996

- Employment Equality (Age) Regulations (Northern Ireland) 2006
- Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000
- Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002
- The Disability Discrimination (Northern Ireland) Order 2006
- The Employment Relations (Northern Ireland) Order 2004
- Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006
- Employment Relations (Northern Ireland) Order 2004 ● Work and Families (Northern Ireland) Order 2006

and will use his best endeavours to ensure that in his employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract he promotes equality of treatment and opportunity between:

a. persons of different religious beliefs or political opinions
b. men and women or married and unmarried persons
c. persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)
d. persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)
e. persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)
f. persons of different ages
g. persons of differing sexual orientation

2.3.2 The Supplier will take all reasonable steps to secure the observance of clause 2.3.1 of this Schedule by all Supplier Staff.

2.4 Equality policies and practices

2.4.1 The Supplier will introduce and will procure that any Subcontractor will also introduce and implement an equal opportunities policy in accordance with guidance from and to the satisfaction of the Equality Commission. The Supplier will review these policies on a regular basis (and will procure that its Subcontractors do likewise) and the Customer will be entitled to receive upon request a copy of the policy.

2.4.2 The Supplier will take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in clause 2.3 above). These steps will include:

a. the issue of written instructions to staff and other relevant persons
b. the appointment or designation of a senior manager with responsibility for equal opportunities
c. training of all staff and other relevant persons in equal opportunities and harassment matters
d. the inclusion of the topic of equality as an agenda item at team, management and staff meetings

The Supplier will procure that its Subcontractors do likewise with their equal opportunities policies.

2.4.3 The Supplier will inform the Customer as soon as possible in the event of:

A. the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or

B. any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its Subcontractors during the Call-Off Contract Period by any Industrial or Fair Employment Tribunal or court,

The Supplier will take any necessary steps (including the dismissal or replacement of any relevant staff or Subcontractor(s)) as the Customer directs and will seek the advice of the Equality Commission in order to prevent any offence or repetition of the unlawful discrimination as the case may be.

2.4.4 The Supplier will monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and will provide an annual report on the composition of the workforce and applicants to the Customer. If the monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier will review the operation of its relevant policies and take positive action if appropriate. The Supplier will impose on its Subcontractors obligations similar to those undertaken by it in this clause 2.4 and will procure that those Subcontractors comply with their obligations.

2.4.5 The Supplier will provide any information the Customer requests (including Information requested to be provided by any Subcontractors) for the purpose of assessing the Supplier's compliance with its obligations under clauses 2.4.1 to 2.4.5 of this Schedule.

2.5 Equality

2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

2.5.2 The Supplier acknowledges that the Customer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours to assist (and to ensure that relevant Subcontractor helps) the Customer in relation to same.

2.6 Health and safety

2.6.1 The Supplier will promptly notify the Customer of any health and safety hazards which may arise in connection with the performance of its obligations under the Call-Off Contract. The Customer will promptly notify the Supplier of any health and safety hazards which may exist or arise at the Customer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Contract.

2.6.2 While on the Customer premises, the Supplier will comply with any health and safety measures implemented by the Customer in respect of Supplier Staff and other persons working there.

2.6.3 The Supplier will notify the Customer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Customer premises if that incident causes any personal injury or damage to property which could give rise to personal injury.

2.6.4 The Supplier will comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other persons working on the Customer premises in the performance of its obligations under the Call-Off Contract.

2.6.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Customer on request.

2.7 Criminal damage

2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Customer for any loss arising
directly from a breach of this obligation (including any diminution of monies received by the Customer under any insurance policy).

2.7.2 If during the Call-Off Contract Period any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.

2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Customer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Customer's cost and the Supplier will (at no additional

cost to the Customer) provide any help the Customer reasonably requires with the appeal.

2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

Schedule 5: Guarantee

Not used

[

.

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform).
Audit	An audit carried out under the incorporated Framework Agreement clauses.
Background IPRs	For each Party, IPRs: • owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes • created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.

Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.

Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.

Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, Personal Data and any information, which may include (but isn't limited to) any: • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.

Controller	Takes the meaning given in the UK GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.

Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
Data Subject	Takes the meaning given in the UK GDPR

Default	Default is any: • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.

ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-todate version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-fortax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.

Force Majeure	A force Majeure event means anything affecting either Party's performance of their obligations arising from any: • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.13 together with the Framework Schedules.

Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or
	defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.

Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.

Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.

Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.

Insolvency event	Can be: • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium • a Dun & Bradstreet rating of 10 or less
Intellectual Property Rights or IPR	Intellectual Property Rights are: • copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information • applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction • all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: • the supplier's own limited company • a service or a personal service company • a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).

IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or Buyer's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.

Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement Schedule 6.
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.

New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.

Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the UK GDPR.

Personal Data Breach	Takes the meaning given in the UK GDPR.
Platform	The government marketplace where Services are available for Buyers to buy.
Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK GDPR.
Prohibited act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.

Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call- Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.

Services	The services ordered by the Buyer as set out in the Order Form.

Service data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controlsche ck-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.

Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.

Supplier staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7: UK GDPR Information

This schedule reproduces the annexes to the UK GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract and clause and schedule references are to those in the Framework Agreement but references to CCS have been amended.

C2 GDPR - MeridianBCMS - State

Annex 1: Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Buyer at its absolute discretion.

1.1 The contact details of the Buyer's Data Protection Officer are: [redacted]

1.2 The contact details of the Supplier's Data Protection Officer are: [redacted]

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, Buyer is the Controller and the Supplier is the Processor of the Personal Data recorded below. The scope of Personal Data which the purposes and means of the Processing by the Supplier is determined by the Buyer: Provision of management tool to store and manage Business Continuity Management Tool member information including consent and contact preferences. **The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: ● Business contact details of Supplier Personnel for which the Supplier is the Controller, Business contact details of any directors, officers, employees, agents, consultants and contractors of the Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under the contract for which the Buyer is the controller.
Duration of the Processing	As set out in this Agreement
Nature and purposes of the Processing	In respect of work email addresses: To allow for communication with employees in respect of the day to day management of business continuity planning for The Customer. In respect of personal mobile numbers: to communicate with employees at time of emergency and or business continuity events.

Type of Personal Data	Personal mobile number, 1st name and second name, work email address.

Categories of Data Subject	NHSBSA Employees
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under UK law to preserve that type of data	All relevant personal data to be deleted or returned to the NHSBSA after the expiry or termination of this Contract unless longer retention is required by Law or the terms of any Call-Off Contract arising hereunder. NHSBSA will retain the personal data in line with the organisation's records retention schedule