

**RM6100 Technology Services 3 Agreement
Framework Schedule 4 - Annex 1
Lots 2, 3 and 5 Order Form**

Order Form

This Order Form is issued in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100 dated 15/06/2021 between the Supplier (as defined below) and the Minister for the Cabinet Office (the "**Framework Agreement**") and should be used by Buyers after making a direct award or conducting a further competition under the Framework Agreement.

The Contract, referred to throughout this Order Form, means the contract between the Supplier and the Buyer (as defined below) (entered into pursuant to the terms of the Framework Agreement) consisting of this Order Form and the Call Off Terms. The Call-Off Terms are substantially the terms set out in Annex 2 to Schedule 4 to the Framework Agreement and copies of which are available from the Crown Commercial Service website <http://ccs-agreements.cabinetoffice.gov.uk/contracts/rm1234>. The agreed Call-Off Terms for the Contract being set out as the Annex 1 to this Order Form.

The Supplier shall provide the Services and/or Goods specified in this Order Form (including any attachments to this Order Form) to the Buyer on and subject to the terms of the Contract for the duration of the Contract Period.

In this Order Form, capitalised expressions shall have the meanings set out in Schedule 1 (Definitions) of the Call-Off Terms

This Order Form shall comprise:

1. This document headed "Order Form";
2. Attachment 1 – Services Specification;
3. Attachment 2 – Charges and Invoicing;
4. Attachment 3 – Implementation Plan;
5. Attachment 4 – Service Levels and Service Credits;
6. Attachment 5 – Key Supplier Personnel and Key Sub-Contractors;
7. Attachment 6 – Software;
8. Attachment 7 – Financial Distress;
9. Attachment 8 - Governance
10. Attachment 9 – Schedule of Processing, Personal Data and Data Subjects;
11. Attachment 10 – Transparency Reports; and
12. Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses.

Section A

General information

Contract Details

Contract Reference:	C21669
Contract Title:	HODC Private IaaS.
Contract Description:	The provision of a private cloud solution and associated services within the Home Office Data Centres.
Contract Anticipated Potential Value: this should set out the total potential value of the Contract	<p>A maximum of £4,050,000 (Initial Term).</p> <p>A maximum of £1,400,000 (Per Extension Period).</p> <p>A maximum of £6,850,000 (Full potential Contract Period).</p>
Estimated Year 1 Charges:	£1,350,000
Commencement Date: this should be the date of the last signature on Section E of this Order Form	22 nd December 2021

Buyer details

Buyer organisation name

The Secretary Of State for the Home Department

Billing address

Your organisation's billing address - please ensure you include a postcode
2 Marsham Street, Westminster, London, SW1P 4DF

Buyer representative name

The name of your point of contact for this Order

Buyer representative contact details

Email and telephone contact details for the Buyer's representative. This must include an email for the purpose of Clause 50.6 of the Contract.

Buyer Project Reference

Please provide the customer project reference number.
C21669

Supplier details

Supplier name

The supplier organisation name, as it appears in the Framework Agreement
Exponential-e Limited

Supplier address

Supplier's registered address
100 Lemon St, London, E1 8EU

Supplier representative name

The name of the Supplier point of contact for this Order
[REDACTED]

Supplier representative contact details

Email and telephone contact details of the supplier's representative. This must include an email for the purpose of Clause 50.6 of the Contract.
[REDACTED]

Order reference number or the Supplier's Catalogue Service Offer Reference Number

A unique number provided by the supplier at the time of the Further Competition Procedure. Please provide the order reference number, this will be used in management information provided by suppliers to assist CCS with framework management. If a Direct Award, please refer to the Supplier's Catalogue Service Offer Reference Number.
[REDACTED]

Section B

Part A – Framework Lot

Framework Lot under which this Order is being placed

Tick one box below as applicable (unless a cross-Lot Further Competition or Direct Award, which case, tick Lot 1 also where the buyer is procuring technology strategy & Services Design in addition to Lots 2, 3 and/or 5. Where Lot 1 is also selected then this Order Form and corresponding Call-Off Terms shall apply and the Buyer is not required to complete the Lot 1 Order Form.

- | | |
|--|-------------------------------------|
| 1. TECHNOLOGY STRATEGY & SERVICES DESIGN | <input type="checkbox"/> |
| 2. TRANSITION & TRANSFORMATION | <input type="checkbox"/> |
| 3. OPERATIONAL SERVICES | |
| a: End User Services | <input type="checkbox"/> |
| b: Operational Management | <input checked="" type="checkbox"/> |
| c: Technical Management | <input type="checkbox"/> |
| d: Application and Data Management | <input type="checkbox"/> |
| 5. SERVICE INTEGRATION AND MANAGEMENT | <input type="checkbox"/> |

Part B – The Services Requirement

Commencement Date

See above in Section A

Contract Period

Guidance Note – this should be a period which does not exceed the maximum durations specified per Lot below:

Lot	Maximum Term (including Initial Term and Extension Period) – Months (Years)
2	36 (3)
3	60 (5)
5	60 (5)

Initial Term Months

36 months

Extension Period (Optional) Months

**Two (2) periods of up to 12 months
Subject to Change Control approvals**

Minimum Notice Period for exercise of Termination Without Cause
(Calendar days) *Insert right (see Clause 35.1.9 of the Call-Off Terms)*

Thirty (30) Calendar days

Sites for the provision of the Services

Guidance Note - Insert details of the sites at which the Supplier will provide the Services, which shall include details of the Buyer Premises, Supplier premises and any third party premises.

The Supplier shall provide the Services from the following Sites:

Buyer Premises:

[REDACTED]

Supplier Premises:

- [REDACTED]
- [REDACTED]

Third Party Premises:

- [REDACTED]
- [REDACTED]

Buyer Assets

Guidance Note: see definition of Buyer Assets in Schedule 1 of the Call-Off Terms

[REDACTED] Laptops

Additional Standards

Guidance Note: see Clause 13 (Standards) and the definition of Standards in Schedule 1 of the Contract. Schedule 1 (Definitions). Specify any particular standards that should apply to the Contract over and above the Standards.

1. Buyer Policies

The Supplier shall follow and conform to all Buyer and HM Government policies, processes and procedures listed below (copies can be found in the Data Library):

1.1 Government policies

- The Government Digital Service Standards:
 - <https://www.gov.uk/service-manual>
- The Government Digital Service Manual
 - <https://www.gov.uk/service-manual>
- Government Digital Service Technology Code of Practice
 - <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
- Government Digital Services Technology Code of Practice – Collection of Related Topics:
 - <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice-related-guidance>
- Government Security Classifications
 - <https://www.gov.uk/government/publications/government-security-classifications>
- General Data Protection Regulations
 - <https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation>

1.2 Buyer Policies - Info security

- Information Assurance Policy

1.3 Buyer Policies - Operating models

- Cyber Security Incident Management Operating Model
- Enterprise Services Portal Operating Model
- Event Monitoring and Management Operating Model
- Incident Management Operating Model
- Problem Management Operating Model
- Release Assurance Operating Model
- Change Management Operating Model
- Knowledge Management Operating Model
- Service Asset & Configuration Management Operating Model
- External Software Asset Management Operating Model
- Risk and Issue Management Operating Model

1.4 Buyer Policies - Business Continuity

- Business Continuity Management policy and guidance
- Business Continuity quick guide
- Business Continuity top tips

1.5 Buyer Policies – Testing



1.6 Buyer Policies – Personnel security

- Security Incidents Policy
- Government Response Level

1.7 Buyer Policies - Cyber security

- Firewall Policy
- Cyber Risk Management Policy
- Cyber Assurance Policy

- Password Policy
- Account Management Policy and Standard

1.8 [REDACTED] Policies – Data Centres Site Security

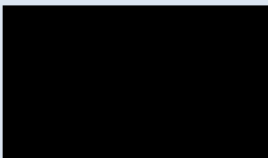
- [REDACTED] security access requirements
- [REDACTED] Site Conduct Guidance

Buyer Security Policy

Guidance Note: where the Supplier is required to comply with the Buyer's Security Policy then append to this Order Form below.

The Buyer's Security Policy comprises the following documents:

- Security Incidents Policy (available in Data Library)
- Government Response Level (available in Data Library)
- Government Security Classifications:
<https://www.gov.uk/government/publications/government-security-classifications>
- General Data Protection Regulations: <https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation>
- Information Assurance Policy (available in Data Library)
- HMG Security Policy Framework:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/710816/HMG-Security-Policy-Framework-v1.1.doc.pdf
- Home Office Security Policy for Contractors:



The nature of the Buyer's business is such that it conducts additional pre-employment checks as part of its personnel security vetting process.

Buyer ICT Policy

Guidance Note: where the Supplier is required to comply with the Buyer's ICT Policy then append to this Order Form below.

- Firewall Policy
- Cyber Risk Management Policy
- Cyber Assurance Policy
- Password Policy
- Account Management Policy and Standard

Insurance

Guidance Note: if the Call Off Contract requires a higher level of insurance cover than the £1m default in Framework Agreement or the Buyer requires any additional insurances please specify the details below.

Third Party Public Liability Insurance (£) - £5,000,000

Professional Indemnity Insurance (£) - £5,000,000

Buyer Responsibilities

Guidance Note: list any applicable Buyer Responsibilities below.

Provision of sufficient access (including provision of escort personnel for supplier DC visits), connectivity, rackspace, power, heat, and related environmental conditions to enable the supplier to install and operate the equipment in the Data Centres.

Provision of suitable Buyer resources (e.g. project, service, technical, commercial, security, etc) to align with the supplier Project & Support teams to ensure that any approvals, processes, documentation, physical or virtual security, and any access requests are provided and/or progressed in a reasonable and timely manner.

Provision of a Security Aspects Letter confirming the [REDACTED] security requirements for the service.

Provision of Connectivity between the Supplier equipment and the Home Office network at each of the DC's (as detailed within Section 4 of the Specification v2.0)

Provision of any required IP address ranges.

Goods

Guidance Note: list any Goods and their prices.

Not applicable.

Governance – Option Part A or Part B

Guidance Note: the Call-Off Terms has two options in respect of governance. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is limited project governance required during the Contract Period.

Governance Schedule	Tick as applicable
Part A – Short Form Governance Schedule	<input checked="" type="checkbox"/>
Part B – Long Form Governance Schedule	<input type="checkbox"/>

The Part selected above shall apply this Contract.

Change Control Procedure – Option Part A or Part B

Guidance Note: the Call-Off Terms has two options in respect of change control. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is no requirement to include a complex change control procedure where operational and fast track changes will not be required.

Change Control Schedule	Tick as applicable
Part A – Short Form Change Control Schedule	<input type="checkbox"/>
Part B – Long Form Change Control Schedule	<input checked="" type="checkbox"/>

The Part selected above shall apply this Contract. Where Part B is selected, the following information shall be incorporated into Part B of Schedule 5 (Change Control Procedure):

- for the purpose of Paragraph 3.1.2(a), the figure shall be £50,000; and
- for the purpose of Paragraph 8.2.2, the figure shall be £500,000.

Section C

Part A - Additional and Alternative Buyer Terms

Additional Schedules and Clauses *(see Annex 3 of Framework Schedule 4)*

This Annex can be found on the RM6100 CCS webpage. The document is titled RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5.

Part A – Additional Schedules

Guidance Note: Tick any applicable boxes below

Additional Schedules	Tick as applicable
S1: Implementation Plan	<input checked="" type="checkbox"/>
S2: Testing Procedures	<input checked="" type="checkbox"/>
S3: Security Requirements (either Part A or Part B)	Part A <input type="checkbox"/> or Part B <input checked="" type="checkbox"/>
S4: Staff Transfer	<input checked="" type="checkbox"/>
S5: Benchmarking	<input checked="" type="checkbox"/>
S6: Business Continuity and Disaster Recovery	<input checked="" type="checkbox"/>
S7: Continuous Improvement	<input type="checkbox"/>
S8: Guarantee	<input type="checkbox"/>
S9: MOD Terms	<input type="checkbox"/>

Part B – Additional Clauses

Guidance Note: Tick any applicable boxes below

Additional Clauses	Tick as applicable
C1: Relevant Convictions	<input checked="" type="checkbox"/>
C2: Security Measures	<input checked="" type="checkbox"/>
C3: Collaboration Agreement	<input type="checkbox"/>

Where selected above the Additional Schedules and/or Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.

Part C - Alternative Clauses

Guidance Note: Tick any applicable boxes below

The following Alternative Clauses will apply:

Alternative Clauses	Tick as applicable
Scots Law	<input type="checkbox"/>
Northern Ireland Law	<input type="checkbox"/>
Joint Controller Clauses	<input type="checkbox"/>

Where selected above the Alternative Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.

Part B - Additional Information Required for Additional Schedules/Clauses Selected in Part A

Additional Schedule S3 (Security Requirements)

Guidance Note: where Schedule S3 (Security Requirements) has been selected in Part A of Section C above, then for the purpose of the definition of "Security Management Plan" insert the Supplier's draft security management plan below.

Security Management Plan to be supplied by the Supplier in accordance with Part B (Long Form Security Requirements) to Schedule S3 (Security Requirements).

Additional Schedule S4 (Staff Transfer)

Guidance Note: where Schedule S4 (Staff Transfer) has been selected in Part A of Section C above, then for the purpose of the definition of "Fund" in Annex D2 (LGPS) of Part D (Pension) insert details of the applicable fund below.

Additional Clause C1 (Relevant Convictions)

Guidance Note: where Clause C1 (Relevant Convictions) has been selected in Part A of Section C above, then for the purpose of the definition of "Relevant Convictions" insert any relevant convictions which shall apply to this contract below.

Cyber Crime, Fraud.

Additional Clause C3 (Collaboration Agreement)

Guidance Note: where Clause C3 (Collaboration Agreement) has been selected in Part A of Section C above, include details of organisation(s) required to collaborate immediately below.

Not Applicable

Appendix 1 - Clarifications to the Contract

Clarification Question is related to:					
Document	Requirement #	Page # / Para # /Subsection	Home Office Ref #	Anonymised Bidder's Question	Home Office Response
Appendix B Specification	Product Catalogue	Page 10 Subsection 2.2.2	HOPI001	Similarly to the personalized, t-shirt size Product Catalogue under [REDACTED] would this same Product Catalogue and ability for Home Office staff to create/configure their own [REDACTED] resources (Virtual Machines etc.), also be required, or is this only required for the [REDACTED] platform?	The Buyer would like to be able to offer that service however at the outset we wish to only use the native catalogue capabilities of the products which the Buyer accepts may limit the options available via [REDACTED] given the requirement to deploy [REDACTED]
Appendix B		2.1.7	HOPI002	Do any of the workloads on the current platform need or utilise hypervisor level integration ?	No
Appendix B		2.5.2.2	HOPI003	When will the Technical Architecture Policy referenced in 2.5.2.2 be released ? Does this policy dictate any industry recognised methodology/framework, for example TOGAF, or define the approval gates and organisation, etc. (EG Architecture Board,	The document is undergoing revision and will be available once complete, a date is unknown at this time. The methodology is to align with the Buyer Technical Design Authority governance processes and required artefacts (Context

				Operations Board, Change Board, etc)	Model, Component Model, Deployment Model). Also see HOPI028.
Appendix B		3.2.4.2	HOPI004	What is the expectation for penetration testing this platform, and assuming that it is required, when should it take place?	[REDACTED]
Appendix B		3.2.20	HOPI005	Can you expand on the definition of the ITOC/ CSOC, specifically: - What processes need to be followed? - Are there any collectors/ agents that require to be installed to support this tooling? - What data/ tools are available from ITOC and CSOC to support the delivery of the platform SLA?	ITOC – IT Operations Centre (first line support) CSOC – Cyber Security Tooling and process info will be communicated to the Supplier following contract commencement due to the sensitive nature of this information.

Appendix B		3.1.3.8	HOPi006	The exemplar programme (at 2.7.2) does not allow 12 weeks for the installation of structured cabling that supports the design. Is there any ability to expedite cabling installation to match the requirement?	The exemplar assumes that the structured cabling requirements will be provided in week 1 (as per the milestone deliverables) and that the cabling will be completed before or during the exemplar “install and configure” milestone
Appendix B		2.5.2.5	HOPi007	Can an estimated timeframe be provided for navigating the governance process for each gate?	If the required artefacts for each gate are accepted the estimated timescale is 2 weeks
Appendix B		2.4.1	HOPi008	Is the networking between DC1 and DC2 in scope ?	No
Appendix B		2.4.1	HOPi009	Where is the network boundary between what is in scope and what is provided already in the DC ?	The Buyer expects the boundary to be the switching supplied as part of the Private IaaS Platform.
Appendix B		2.4.1	HOPi010	Is there a network route available within DC1/DC2 for remote management i.e. internet + switch routing? Or is it possible to establish a private connection from elsewhere [REDACTED]	[REDACTED] [REDACTED]

Appendix B		2.1.3	HOP1011	The requirement asks for 'the Supplier shall provide 24/7 Level 4 Support'. What is the assumption of the Buyer organisation's role in Levels 1 to 3? How does this align with the desire for provision 'as a service' (2.1.4)?	The Buyer has a Hosting Capability supplier who will be the primary support vehicle for Buyer data centre operations. The expectation is that the Supplier will provide assistance to that Capability Supplier where required. Given that the Capability Supplier has expertise in both required platforms it is expected that the Supplier will only be required for complex issues, commensurate with a "Level 4" support tier.
Appendix B		2.6	HOP1012	Is there a Home Office build standard that VM templates should conform to ? Hardening etc	Yes
Appendix B		3.1.3.9	HOP1013	What is provided as part of the rack install ? For example, does it include any TOR switches or standard cabling ?	The rack is supplied with dual PDU and TOR switching can be included - cabling has to be requested to meet requirements.
Appendix B		3.1.3.11	HOP1015	In the aisles that might be used for the Private IaaS, how much kWh is available for the Private IaaS platforms once	This data cannot be provided

				existing racks and their contents are factored in ?	
Appendix B		3.2.4.2	HOP1016	What backup products do the buyer use ? And how are they currently integrated ?	This data cannot be provided but it can be expected to be a standard backup application with capabilities to back up both hypervisor and guests
Appendix B		4.1.6	HOP1017	What facilities exist within HODC1 and HODC2 for unboxing and racking hardware ? Is there a build room for example ? How long can equipment be stored before racking if required?	There are client rooms that can be used as office space, there is limited storage and the expectation is most deliveries are on a "just in time" basis to minimise the need for on site storage. Build activity can be done at the rack.
Appendix B		6.4.1	HOP1018	What is the Buyer's Monitoring and Alert Tooling ?	This will be provided after contract award.
Appendix B		6.4.1.3	HOP1019	How does the Buyer's Monitoring and Alert Tooling integrate with the Buyer's SIEM tooling ?	<div style="background-color: black; width: 100%; height: 1.2em; margin-bottom: 2px;"></div> <div style="background-color: black; width: 100%; height: 1.2em; margin-bottom: 2px;"></div> <div style="background-color: black; width: 100%; height: 1.2em;"></div>
Appendix B		3.2.6	HOP1021	3.2.6 and 3.2.7 use the term "functions" - are these the functions defined in 2.2.2?	In 3.2.6 and 3.2.7 we are referring to platform functionality, not referring to business functions listed in 2.2.2

Appendix B		4.1.6	HOP1022	Is there an SLA for access approvals to the DC's	Yes
Appendix B		2.7.2	HOP1023	Can you provide planned change freeze periods that may impact implementation during the duration of the project	This data cannot be provided at this point in time. The Buyer may be able to make exceptions for additive / non-disruptive work
Appendix B		2.4.1	HOP1024	Do you have any indication of latency between DC1 and DC2 ?	No
Appendix B		4.4	HOP1025	As Framework Schedule 4, Annex 3, Schedule S1 states 20 days to approve the Detailed Implementation Plan, will the buyer be able to approve the design deliverables earlier to enable Hardware & Software to be ordered?	The Buyer will consider fast tracking the design approval process
Appendix B		Further Competition Initiative (4.1)	HOP1026	Will notification of Contract Award take place ahead of commencement date to enable time for resources to be mobilised	Due to the compacted nature of the procurement there will be little gap between the 2 dates however notification will occur prior to commencement

Appendix B		6.1.1.7	HOP1027	Service Incidents must be raised "on-tool" via Buyer's Service Management Tool - will this (and wider use of Buyers toolsets required elsewhere) require the use of [REDACTED] laptops?	Yes
Appendix B		para 2.5.2.5	HOP1028	Para requests compliance with "ES Technical Architecture governance process" but this is not a referenced document nor can I see it in the data room. Please provide a copy of the correct version.	The ES Technical Governance process is currently being redesigned. "Enterprise Services Architectural Governance Flow.jpg" shows the proposed flow diagrammatically (the file has been added to the data library to be shared with bidders)
Appendix B		general	HOP1029	Please provide the 'functional' and 'non-functional' design requirements for the Private IaaS platform to enable solution design and adherence.	Please clarify providing examples

Appendix B		general	HOP1030	Please provide the demarcations of ongoing service requirements between the Private IaaS provider and the Hosting Capability Provider (ideally a RACI) as requirements appear to substantially overlap and/or be duplicated.	The production of a RACI is a requirement on the Supplier of the design as per section 3.2
Appendix B		Section 2.6 - Software Licencing	HOP1031	Please provide the volumes and types of existing software licenses that the Buyer intends to re-use, and the split between those reused on [REDACTED] and [REDACTED]	The Buyer considers the licences required for the Private IaaS Platform to be in scope and therefore does not assume re-use of existing licencing
Appendix B		Section 2.5.2	HOP1032	Please provide the Buyer Design Standards that the Private IaaS platform will need to adhere to	See HOP1028
Appendix B		Section 3.2.12	HOP1033	Please provide the requirements for Test environment(s)	Section 3.2.12 does not reference a test environment, please clarify
Appendix B		3.2.4.2 (g)	HOP1034	Please detail the Buyer's backup product and configuration which will need to be integrated with the suppliers solution.	See HOP1016

Appendix B		6.2.5	HOP1035	Please provide details of the requirements for off-site data backup and related retention period?	There are requirements for the configuration to be backed up and maintained in order to meet the required parameters of section 6.2.5. No requirement exists for this to be offsite or retained long term
Appendix B		4.2.4	HOP1036	Please provide details for the existing Cloud Providers provisioning systems?	The Buyer uses the [REDACTED] and requires that the [REDACTED] provided as part of the Private IaaS Platform is integrated into this portal
Appendix B		4.2.7	HOP1037	Please provide details of the sample source workloads to migrate and what the workloads may consist of?	The Buyer will detail virtual workloads that are analogous to live workloads. This will consist of virtual machines running multiple operating systems and virtual appliances
Appendix B		4.2.8	HOP1038	Please provide details of the sample source workloads to transform and what the workloads may consist of?	The Buyer will re-use the workloads from section 4.2.7 and is aware that for [REDACTED] this may introduce an element of transformation

Appendix B		2.7.1	HOP1039	Can the Buyer please provide the workload requirements for intensive GPU operations in addition to the vCPU requirements specified in the ITT for both the [REDACTED] and [REDACTED] solutions?	There are none
Appendix B		6.2.5	HOP1040	Can the Buyer please provide the requirements for off-site data backup and the retention periods?	[REDACTED] [REDACTED]
Appendix B		3.2.10	HOP1041	Can the Buyer please describe the functional and non functional tests required to validate migration or transformation from the new [REDACTED] platform to the new [REDACTED] platform (and/or vice versa)?	These are to be defined as part of the design process
Appendix D Pricing Model	Pricing	Solution Details TAB Cell G98	HOP1051	Is the formula incorrect. We are assuming this is supposed to be dividing by 3 due to the 3:1 contention Ratio, However it is only dividing F55 by 3 and not C55 as the C55+F55 need to be in brackets before dividing by 3. Should the formula be =(C55+F55)/3	This is correct, corrected spreadsheet attached - Please refer to this as the final document

Appendix B		3.1.3.9	HOP1014	Are there any empty racks already in situ within DC1 and DC2 that can be used ?	Capacity exists in HODCx for additional racks , as per requirements full details of the equipment needed to confirm space reservations.
Appendix B		5.1.1.2	HOP1020	Much of each platform could be defined as "data bearing". Please define what is meant in this context.	There is an error in section 5.1.1.2 - this should read "Any data bearing component of the Private IaaS Platform will be retained by the Buyer." Due to the sensitivity of the data held on the Private IaaS Platform the Buyer must retain all data bearing hardware for secure destruction which is replaced for maintenance or any other reason. Such components cannot be returned to the Supplier at any time.

Appendix B		6.1.1.7	HOP1042	Service Incidents must be raised "on-tool" via Buyers Service Management Tool - will this (and wider use of Buyers toolsets required elsewhere) require the use of [REDACTED] laptops?	See HOP1027
2.6			HOP1043	Can more detail be provided on template requirements ? OS versions, VM types - DB, Web etc	See HOP1037
3.2.2			HOP1044	Can suppliers perform their own discovery, using their own tools ? or is this just an analysis of a provided [REDACTED] output ?	It is unlikely that discovery tools will be permitted therefore the expectation is that the output of a more up to date and complete [REDACTED] report will be the basis for migration

4.4			HOP1045	Some of the deliverables can be provided within 30 days (6 weeks) of commencement date, however the milestone date for Design M2 is 4 weeks after Commencement date. Please can this be clarified?	The Buyer assumes that there will be further refinement of the documents listed as required within 30 days and expects the milestone date to be achieved with interim draft copies of those documents
3.2.3.1			HOP1046	The Framework states that the Detailed Implementation Plan is produced using a software tool as specified, or agreed by the Buyer. Please can you confirm what tool will be applicable in this case?	The software tool applicable will be Microsoft Project
			HOP1047	Based on the provided [REDACTED] output, the quantities of vCPU, RAM and Storage are approx. the same as that requested in the MVP pricing. During a DR event where one site is inoperable, do all VMs need to be available in the alternate DC ?	[REDACTED]

6.2.5.4			HOP1048	What is the definition of a Virtualised Asset ? Does this encompass the buyer's workload VMs ?	Virtual Asset is any virtual appliance or tool which exists to provide the Private IaaS Platform. It does not include any Buyer workload virtual machines
6.2.5			HOP1049	Are applications hosted on the current platform architected across both Home Office DCs ? In the event of losing a DC, do the applications still function ?	Yes, Buyer applications are architected in this way
			HOP1050	In addition to the supplied ██████ output, would it be possible to supply the number of discreet applications supported by the listed virtual machines?	Due to the sensitive nature of the applications hosted on this platform this information cannot be shared. It will be made available from commencement date

Appendix B Specification	Specification	Page 13 Subsection 2.4	HOP1052	How many VMs in total will be provisioned on the new systems?	The number of virtual machines will change over the contract term. The Buyer expects a flexible platform which can accommodate such changes. It is expected that at commencement date there will be approximately [REDACTED]
Appendix B Specification	Specification	Page 18 Subsection 3.2.4.2	HOP1053	What is the buyers backup product that we will need to integrate with?	The Buyers backup product will be one that can support integration with both [REDACTED] and [REDACTED]
Appendix B Specification	Specification	Page 18 Subsection 3.2.4.2	HOP1054	Is it the intention to utilise the buyers backup software for both the [REDACTED] platform as well as the [REDACTED] platform?	Yes

Appendix B Specification	Specification	Page 33 Subsection 6.2.5	HOP1055	In order to manage RPO & RTO are we utilising the buyers Disaster Recovery software ? (if so what is it please), or as the Supplier are we providing this as part of the solution? If the Supplier is providing the DR software please can you confirm the number of VMs requiring protection.	The Supplier is required to maintain the requirements for any element (virtual or physical) which forms part of the Private IaaS Platform. Buyer workload virtual machines do not need to be considered for this requirement
Appendix B Specification	Specification	Page 33 Subsection 6.2.5	HOP1056	Please can you supply a RACI of ownership of tasks with regards to both backup and disaster recovery, as there is likely to be lots of overlapping responsibilities between the buyer, the suppliers of the OS & App service and the supplier of this private cloud provision. i.e. many systems are either protected at the Hypervisor layer or software layer and sometimes both, in order to achieve 99.99% availability	See HOP1030

Appendix B	4.1.2	Page 21 / Appendix B	HOP1061	[REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED]
Appendix B	2.1.1 / 4.1.13	Page 8 & Page 21 / Appendix B	HOP1062	Additional Software: Is the new provider expected to provide their own software BOM for [REDACTED] [REDACTED] or will this be supplied by The Department.	The Buyer expects the solution pricing to include [REDACTED] licencing
Appendix D			HOP1063	The sizing calculation in cells G98 and G108 on the solutions details tab seem to be incorrect. Both cells should be dividing the entire sum by 3, to represent the contention ratio requested.	An updated version of the spreadsheet has been released to the portal which corrects this error

Appendix B		3.2.2	HOP1064	If supplier can complete their own discovery, how quickly can access to be provided?	The supplier is unlikely to be able to complete their own discovery, access will not be provided
Appendix B		2.6	HOP1068	"Migration of Buyer Virtual Workloads" - how long does the buyer envisage the migration of workloads onto the platforms will take from a start date of the end of May 2022? Will this be influenced by retirement of the existing [REDACTED] platform, and if so, what is the end date for migrations to have been completed by?	The Migration of Buyer workloads is not within scope for this procurement. The requirement for the platform to be available for the migration of workloads to commence remains as stated
Appendix B	3.2.5 / 3.2.5.1 / 3.2.5.2	Page 18 / Appendix B	HOP1057	Commitment. Are we to understand that : A, the authority wants to commit to reserving 90% of the Hardware available to use but wants variable pricing on 10% burst? Or B, are we to understand that the authority wants to commit to reserving 70% MVP and wants variable pricing on	The Buyer may choose to commit for 100% of the MVP platform which will as per the requirements include >= 20% surplus capacity. The Buyer expects the price provided for this commitment level will include the required 10% burst capacity.

				30% (20% surplus plus 10% burst).	
Appendix B	3.2.5.1 / 3.2.5.2	Page 18 / Appendix B	HOP1058	End of Contract: Does the Surplus and Burst apply to the Month 36 requirements as detailed in the Potential Future Platform Growth.xlsx	The Buyer wishes to maintain 20% surplus and 10% burst through the contract via acquisition of scale units
Potential Future Platform Growth.xls	3.2.5.1 / 3.2.5.2	All column F	HOP1059	End of Contract: Will there be any possibility of growth above the projections between months 24 & 36	The possibility exists that the projections may be higher or lower than those shown in the spreadsheet

Potential Future Platform Growth.xls	3.2.5.1 / 3.2.5.2	Various columns (all)	HOP1060	Additional capacities : Is the 36 month term from the start of the contract award or from the installation of additional capacities i.e. is month 1 the start of the contract or month 1 the start of additional capacity	36 Month term starts upon counter-signature of the Call-Off Contract.
Appendix C		5.4	HOP1065	The guidance advises to include a risk register with the following attributes "category, impact, severity, probability, risk rating and mitigation strategy". Some of these are in addition to the Risk Register format that has been requested in under 3.10, so should we provide a separate document or are we permitted to add the additional columns to aforementioned Risk Register	The Potential Providers are to amend the Risk Register under 3.10 to include the additional data.
Appendix A		Section C, Part A	HOP1066	Is staff transfer assumed to be applicable to this engagement?	This is a new service with no incumbent supplier and no Home Office staff providing the services.

Appendix A		Section C, Part A	HOP1067	When will the Authority release extent and details relating to any applicable staff transfer?	This is a new service with no incumbent supplier and no Home Office staff providing the services.
			HOP1069	Is the support up to the hypervisor (only bare metal) or including the hypervisor such as [REDACTED]	The requirements are as stated and include both the bare metal and hypervisor options stated in addition to all other requirements
			HOP1070	[REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED]

Appendix B		6.1.1.7	HOP1071	Can the buyer confirm if there is an SLA on [REDACTED] accounts and laptops from the point of request to typical setup and handover for a user. If no SLA exists please confirm the average lead time.	"The average lead time for [REDACTED] Laptop request initiation to fulfilment is fifteen (15) working days." The impacts on the lead time can be managed throughout the process.
Appendix B		6.1.1.7	HOP1072	Can the buyer confirm if the [REDACTED] tooling would be able to be configured to also email to a resolver group (on the suppliers external email address) for Incidents / Requests / Problems / Changes when assigned to the suppliers resolver group?	Subject to security assurance, the [REDACTED] tooling can be configured to email an external address when assigned to the supplier resolver group
Pricing Schedule			HOP1073	We have inputted our Supplier recommended split under tab "Solutions Details" - "Baseline Requirements, Section 1". We've entered our proposed distribution into the yellow boxes rows 55-65. We had expected these would dynamically update the scenarios to reflect the proposed distribution as per the "Potential Future Growth" spread sheet provided under the Data Library. Instead we've	There is an error on scenario 1 , a corrected version is attached (v4.0) For scenario 2 we specify the growth of each platform and the intention is that they should accept the values as proposed (we do not calculate the growth on the back of what their proposed distribution is). Only service periods 1 – 11 will reflect their proposed distribution. For scenario 3

			noticed that from Period 2 onwards its using the fixed growth figures from the "Potential Future Growth" spread sheet, not the suggested distribution split as reference above. This is occurring across all 4x scenarios. Can you please confirm if this is intentional?	and 4 it does and should use the figures they enter for the breakdown and on ourcopy that is what is happening – if the Potential Provider can supply a screenshot of what they are seeing that would be useful if the new version does the same for them
--	--	--	---	---



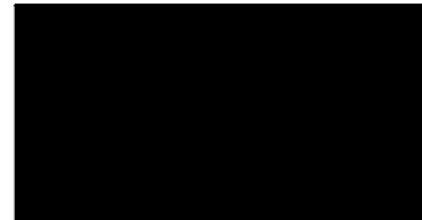
Section E

Contract Award


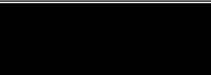
This Call Off Contract is awarded in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100.

SIGNATURES

For and on behalf of the Supplier

Name	
Job role/title	
Signature	
Date	22 ND DECEMBER 2021

For and on behalf of the Buyer

Name	
Job role/title	Commercial Manager
Signature	
Date	23/12/21

Attachment 1 – Services Specification

1. INTRODUCTION

1.1. This document

- 1.1.1. This Specification and Requirements document relates to the Further Competition to award a Call Off Contract for a Private IaaS Platform Supplier to a sole supplier.
- 1.1.2. This Further Competition is being conducted under the CCS Technology Services 3 Framework Agreement (reference RM6100) Lot 3b.
- 1.1.3. This Specification and Requirements document (ITT Appendix B) contains detail of the services the Supplier will be required to supply to the Buyer in accordance with the Contract.

1.2. Background to the Buyer

- 1.2.1. The Home Office is one of the original great Departments of State and has one of the most challenging jobs in government. Its mission is fundamentally important: to keep Britain safe and secure.
- 1.2.2. The Home Office mission is to deliver a safe, fair and prosperous UK via 4 priorities:
 - Restore confidence in the criminal justice system
 - Attract talent and take back control
 - Protect homeland security
 - Advance Britain's place in the world
- 1.2.3. The Home Office leads on immigration and passports, drugs policy, crime policy, counter-extremism and counterterrorism and works to ensure visible, responsive and accountable policing in the UK.
- 1.2.4. The Digital, Data and Technology (DDaT) function within the Home Office is at an exciting point of evolution. Since 2010, the delivery of technology services within the UK government has been radically transformed, with major changes implemented to enable departments to take back increased control of the design, build and/or operation of their key technology services.

- 1.2.5. DDaT is made up of 1800 Civil Service staff, augmented by a further 2700 contractors and many supplier partners. Every year, our systems support over 3 million visa applications, checks on 100 million border crossings, 5 million passport applications and 140 million police checks on people, vehicles and property. Many of these services support critical national functions and contain sensitive public information.
- 1.2.6. Within DDaT, the Enterprise Services (ES) teams are responsible for delivering common infrastructure services (not applications) that are consumed by multiple Home Office business Portfolios; for example, HM Passport Office (“HMPO”) and Borders. The ES team are supporting and enhancing services in a complex and demanding operational multi-supplier environment whilst at the same time delivering service transformation.
- 1.2.7. In 2016, the Home Office began using the [REDACTED] [REDACTED] its strategic Data Centre capability (HODCx) and in 2018, ES awarded the running of the infrastructure located in HODCx to a supplier. ES continued refining and maturing the infrastructure and services offered out of these Data Centres over time including separating [REDACTED] and [REDACTED] Security domains and invested in key service improvement activities targeted at improving service quality, service commonality and overall service availability.
- 1.2.8. In HODCx, programs of work are refreshing infrastructure foundational services to remove technical debt. This will pave the way for a wider infrastructure transformation program to coincide with natural refresh junctions.

1.3. **Background to the Requirements**

- 1.3.1. The Buyer has commercial arrangements with a supplier to provide 24/7 maintenance and infrastructure delivery capabilities for Private Cloud. This Contract is to compete for a new Private IaaS Platform. The maintenance and operation of the extant Private Cloud will remain with its incumbent supplier and does not form part of this Appendix B (Specification and Requirements).
- 1.3.2. The Buyer’s strategic direction is to continue the digital transformation of services, adopt innovative technologies, provide secure hosting services for Workloads of an [REDACTED] classification based on a consumption model, and support for on premise infrastructure (on-premise and private cloud) in HODCx.
- 1.3.3. The Buyer’s key strategic principles are:
- Technology convergence
 - Shared technology products

- Becoming product centric
- Becoming data driven
- Effective delivery
- Effective innovation

1.3.4. A new single Contract for a Private IaaS Platform Supplier is required with a sole supplier to provide provisioning of infrastructure, configuration, maintenance, expansion and Upgrade capabilities over the next 3 to 5 years (3+1+1). This document provides the specification and requirements for the new Service.

2. HIGH LEVEL REQUIREMENTS AND SCOPE

2.1. Objectives

The main objective is to fulfil the Digital Data and Technology (DDaT) strategy for on-premise [REDACTED] Private IaaS capability.

...A Private Cloud service offering is needed with the ability to support multiple tenants securely to deliver the capabilities, technology, management and processes required to support the business needs of the organisation and provide business value as needed for the delivery of 'Private Cloud' services.

- 2.1.1. Currently this strategy is fulfilled by a [REDACTED] [REDACTED] deployment. This deployment was implemented in 2015 and is reaching the end of its life. Since 2015 the above strategy has been defined and we now require a consolidated platform that can be Scaled to be consumed by projects and portfolios across the organisation as needed.
- 2.1.2. The Supplier shall maintain 99.99% Availability for the Private IaaS Platform. As the Supplier is not responsible for the Workloads, the availability shall only be measured from a Platform Level.
- 2.1.3. The Supplier shall provide a service to match the commitments of our incumbent hosting supplier and therefore the Supplier shall provide 24/7 Level 4 Support of the Private IaaS Platform.
 - 2.1.3.1. The Supplier shall be responsible for ensuring that the 99.99% Availability of the Private IaaS Platform is maintained.
 - 2.1.3.2. The Supplier shall ensure through effective review and management that any agreements required from the Buyer or the Buyer Third Parties to ensure the required Availability are maintained.
 - 2.1.3.3. The Supplier shall participate in the creation of failure scenarios for monitoring the Availability of the Private IaaS Platform that the Buyer may in future develop through improved capability and revised tooling.
 - 2.1.3.4. The Buyer reserves the right to reduce the Service Level Availability of [REDACTED] [REDACTED] and/or [REDACTED] via contract change notice to 99.9% as per the information provided in the Pricing Model.
- 2.1.4. The Supplier shall provide a consumption based Private IaaS solution delivered using an "as a service" model to facilitate maintenance, scalability and renewal at a predictable cost.

- 2.1.5. The Supplier shall ensure that the underlying hardware platforms will be composed of Hyper-Converged Infrastructure (HCI). The Buyer wishes to make use of infrastructure that can support the concept of Scale Units with the ability to Scale up and Scale down to meet current and future business demands.
- 2.1.6. The requirement for [REDACTED] is based on a strategic aim to extend the Buyer's cloud capabilities whilst maintaining the aspects of on-premise Private IaaS deployments the Buyer requires. The choice of [REDACTED] was made due to its mature Product Catalogue for commonly requested services and its alignment with the Buyer's existing cloud automation.
- 2.1.7. The requirement for [REDACTED] [REDACTED] is to provide a platform which offers broad compatibility with incoming Workloads from future inbound migrations and [REDACTED] Workloads currently hosted in HODCx which are not suitable for [REDACTED] or other forms of transformation.

2.2. Product Centric Outcomes

- 2.2.1. A key theme within the DDaT function is the organisational transformation of how the Buyer delivers its services to the Home Office. The Buyer is currently delivering a major program of works which is instrumental in framing and driving this transformation. This program is called Networks and Infrastructure Capability Program (NICP) and reaches across the whole function.

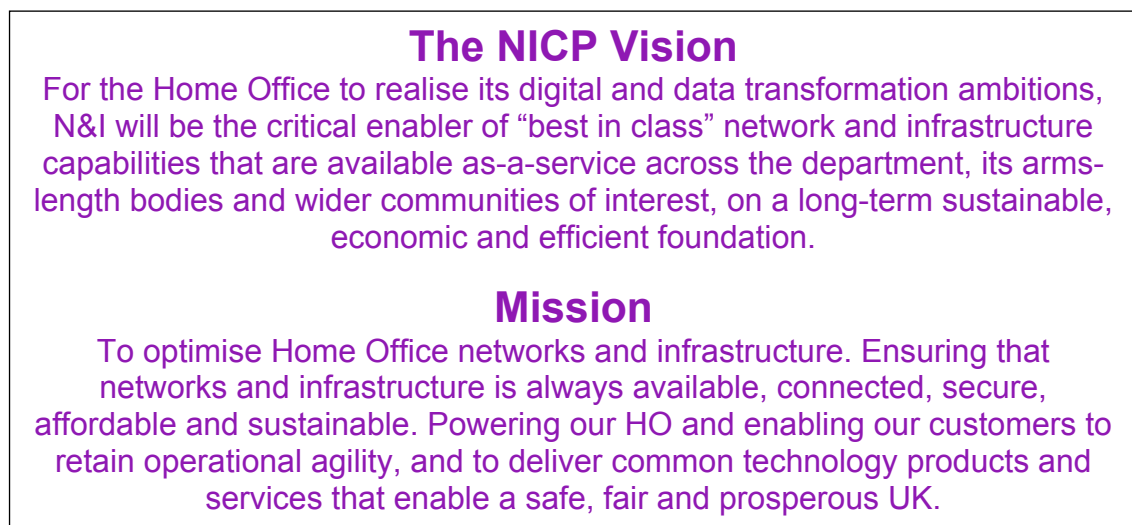


Figure 1 - Product Centric Delivery Model

- 2.2.2. The Private IaaS Platform will provide capability which enables the following functions:

2.2.2.1. Product Engineering

- a) The Buyer intends to leverage the out of the box product capability of the Private IaaS solution to enable the following features as a minimum:
 - i) Creating templated infrastructure products (e.g. T-shirt size VMs, database-as-a-service)
 - ii) Product Catalogue to offer self-service access to both default and custom templates
- b) Product development and automation
- c) Refining Product Catalogue

2.2.2.2. Service Operations

- a) Critical to maintaining all Service Levels and performance targets
- b) Capacity and Billing management (Showback/Chargeback)

2.2.2.3. Service Engineering

- a) This is the Supplier function responsible for delivering resolutions to technical issues that cannot be Resolved by Service Operations
- b) Optionally maintain infrastructure via evergreening solution

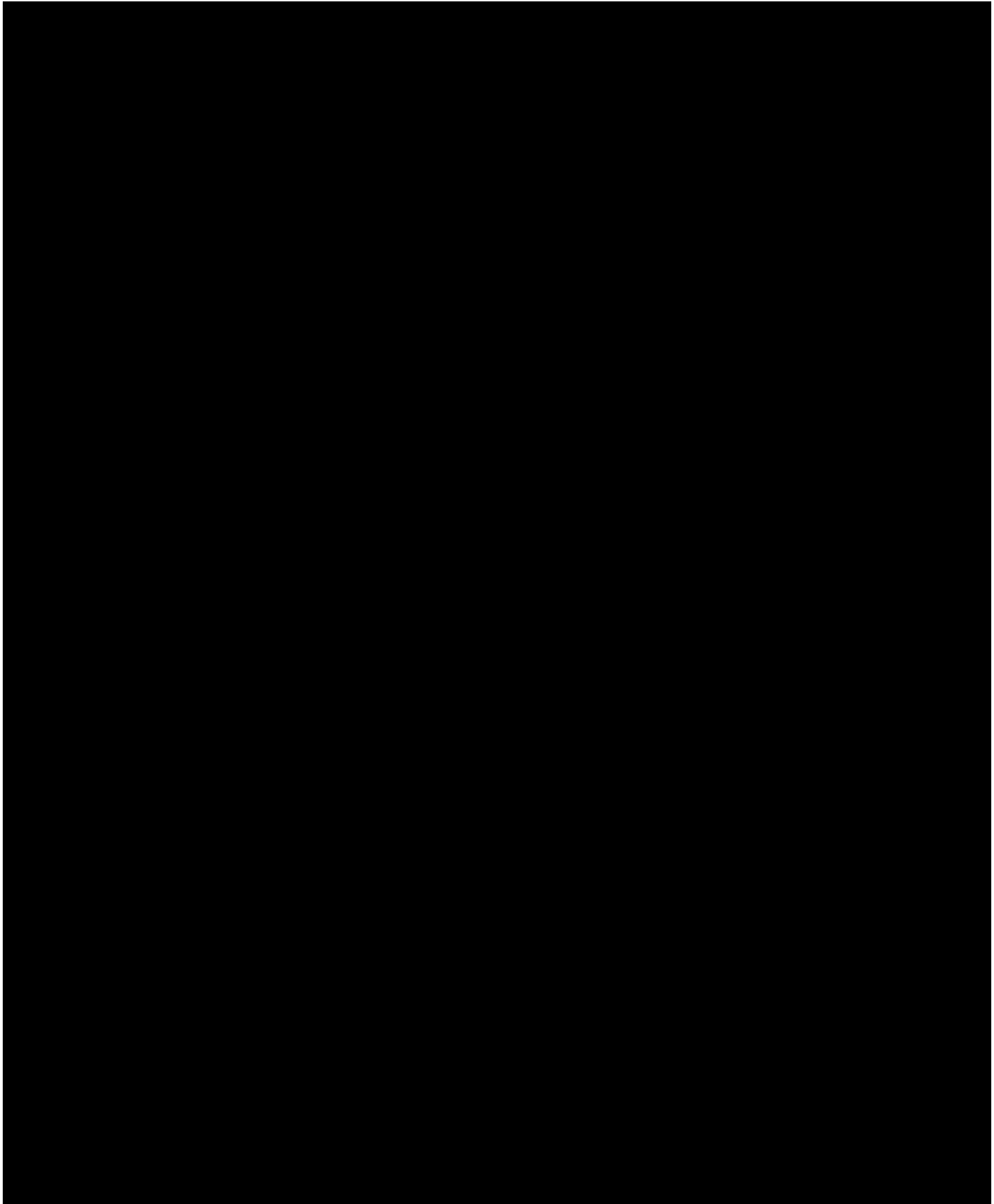
2.3. Supplier Characteristics and Behaviours

2.3.1. The Supplier shall (this is not an exhaustive list):

- 2.3.1.1. Work collaboratively with the Buyer and the Buyer's Third Parties
- 2.3.1.2. Work pro-actively with the Buyer and the Buyer's Intelligent Hands and Hosting Capability Providers in a spirit of trust and mutual confidence
- 2.3.1.3. Co-operate with the Buyer and the Buyer's Third Parties to enable the efficient delivery and operation of Private IaaS
- 2.3.1.4. Assist in sharing information with the Buyer and the Buyer's Third Parties for the purposes of facilitating adequate provision of the Services.
- 2.3.1.5. Agree service hand-offs across Supplier boundaries
- 2.3.1.6. Provide joint problem solving and resolution of problems
- 2.3.1.7. Collaboratively participate in multi-Supplier change boards and move to modern release-based controls over time
- 2.3.1.8. Assist the Buyer in driving innovation to reduce cost, improve service and ensure diversity of service
- 2.3.1.9. Work with the Buyer's Assurance and 3rd party assurance leads to ensure an acceptable level of compliance and improvement

2.4. High Level Technical Scope

- 2.4.1. The high-level technical scope of the Private IaaS Platform is detailed in *Figure 1 – High-level Technical Scope* and will hereafter be referred to as the Private IaaS Platform. Further lower level details of the existing Workloads are provided in the Data Library.



2.5. High Level Call Off Contract Components

2.5.1. The Contract has 4 distinct components which are summarised below:

- Design and design patterns of Private IaaS and Service operational Model development
- Implementation, Testing and Acceptance
- Ongoing Maintenance, Scalability and Upgrades
- Service Management

2.5.2. Design

2.5.2.1. For the design component of the Contract, the Supplier shall align to key themes of the Buyer's Target Operating Model, these are

- Reduction in manual processes
- Increased automation
- Extended Product Catalogue offering
- Improved productivity
- Reduced TCO

2.5.2.2. The Supplier shall follow the Buyer approved methodology for Technical Architecture (Policy to be released).

2.5.2.3. The Supplier shall provide a full set of Architectural Artefacts to include, as a minimum, a context model, component model (high level design), service design, deployment model (low level design), test design, test plan and a delivery plan.

2.5.2.4. The Supplier shall work with the ES Technical Architect team and follow Buyer governance models including both Architectural Discussion Forums (ADF) and Technical Design Authority (TDA) forums.

2.5.2.5. The Supplier shall ensure that the design successfully completes the ES Technical Architecture governance process in order for acceptance to be validated.

2.5.3. Implementation, Testing, Acceptance and Handover

2.5.3.1. The Supplier shall provision and implement the Service to the agreed design.

2.5.3.2. The Supplier shall complete testing in accordance with Schedule S2 (Testing Procedures).

- 2.5.3.3. The Supplier shall seek acceptance of the implementation, capturing and resolving any issues identified.
- 2.5.3.4. The Supplier shall produce documentation and perform handover to the Hosting Capability Provider.

2.5.4. Ongoing Maintenance, Expansion and Upgrade

- 2.5.4.1. The Supplier shall provide 24/7/365 support of the Private IaaS Platform to the Buyer and their Third Parties.
- 2.5.4.2. The supplier shall engage with the Buyer and their Third Parties to Scale the Service under this Contract.
- 2.5.4.3. The Supplier shall provide capability Upgrades to enhance the Service.
- 2.5.4.4. The Supplier shall engage in transition activities requested by the Buyer as part of any change of Hosting Capability Provider.

2.5.5. Service Management

- 2.5.5.1. The Supplier shall perform all requirements defined in Section 6.

2.6. High Level Contract Scope

In Scope	Out of Scope
[REDACTED] platform in Home Office [REDACTED] HODC1 and HODC2	Other [REDACTED] platforms in Home Office [REDACTED]
Private IaaS Platform Product Catalogue(s)	Hosting Supply and Management (Cloud and On-Premise)
HO-IaaS (Home Office Infrastructure as a Service)	Support for physical Data Centre /co-location services
Home Office and Infrastructure tooling (CSOC and ITOC tooling)	Other Home Office Data Centres services
Support up to and including Platform Level	Data centres Smart Hands service
Creation and maintenance of template images which form part of the provided service	Network infrastructure beyond the switching required for the Private IaaS Platform
Hardware and Software procurement	Management of OS or Buyer template images

Service Upgrades	Application support services
Hardware and Software installation	Management of provisioned O/S
Hardware and Software licencing	Any services as requested to be removed by the Buyer throughout the Contract Period by Change Control Procedure
Hardware and Software Break/Fix	Providing 3rd party assurance
Architectural and Operational Artefacts	Migration of Buyer virtual Workloads
Any services as requested to be added by the Buyer throughout the Contract Period by Change Control Procedure	
Working with and remediating for assurance and security requirements as they occur	

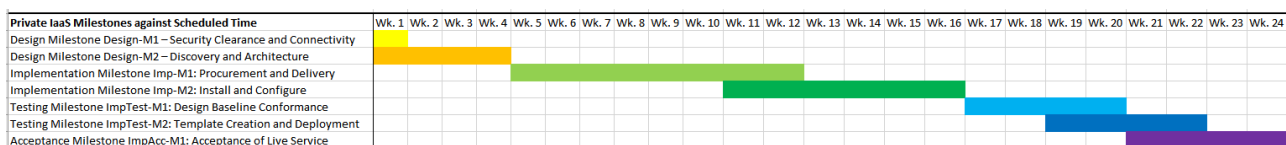
Table 1 - Contract Scope

2.7. Overarching Requirements

2.7.1. The overarching requirements that cover all components of the Contract are:

- An on-premise consumption based Private IaaS Platform capable of cost effectively supporting initial Minimum Viable Product (MVP) Workload requirements which can be Scaled easily to match demand.
- A 99.99% Service Level for Availability of the supplied Private IaaS Platform and associated HCI hardware platform is required for [REDACTED] and [REDACTED] separately in both HODC1 and HODC2. The Availability Service Level must be maintained in a situation where one of HODC1 and HODC2 is not Available.
- All Supplier Personnel shall be Cleared Resources.
- All Cleared Resources to be located within the United Kingdom and all work must be undertaken within the United Kingdom.
- Achievement of Acceptance Milestone ImpAcc-M1: Acceptance of Live Service must complete by the end of May 2022.

2.7.2. The Buyer has detailed the required date for Achievement of the Milestones provided. The timeline shown below is provided as an exemplar.



2.8. Contract Exit

2.8.1. The Initial Term of the Contract is three years.

2.8.2. After the Initial Term, the Extension Periods may be exercised by the Buyer for either one or two further 12-month periods.

2.8.3. The Supplier has provided prices for the hardware acquisition of the Private IaaS Platform. The Supplier shall ensure that the Buyer can request to acquire the hardware infrastructure for the Private IaaS Platform at the prices stated in the Pricing Model.

2.8.4. On the expiry or termination of the Contract, the Supplier shall be responsible for all Supplier exit costs (both identifying and undertaking the agreed exit activities) incurred.

- 2.8.4.1. These activities will include any support handover or change to configuration required to enable the migration or transformation the Workloads on the Supplier provided platforms onto replacement platforms acquired by the Buyer.

3.

3.1.

- ### 3.1.1.

This chapter details the constraints of the physical environment and the requirements of the Private IaaS Platform design.

3.1.2.

3.1.3.

HODC1 and HODC2 have the following constraints:

3.2.

- 3.2.1. The design of the Private IaaS Platform is to be agreed solely by the Buyer. The Buyer has multiple customers and suppliers who are stakeholders in the Private IaaS Platform and therefore the Buyer must perform an Intelligent Client function and represent these stakeholders in the design approval process.
- 3.2.2. The Supplier shall perform a discovery of the Private IaaS solution in use at the Commencement Date. The discovery will be based on an updated Buyer [REDACTED] extract to be provided following the Commencement Date.
- 3.2.3. The Supplier shall provide a Discovery Report detailing the output from the discovery process. This report will include the rationale for the Suppliers decision about platform allocation for the Workloads and any discrepancy identified in the hardware required for the Workloads. This report will be used to inform the agreed design documents. As part of the Discovery Report, the Supplier shall identify compatible destination platforms for each discovered Workload based on the capability and feature set of the respective platforms for validation by the Buyer.
- 3.2.3.1. The Supplier has provided an Outline Implementation Plan which shall be expanded into a Detailed Implementation Plan as per the requirements of Framework Schedule 4, Annex 3, Schedule S1 – Additional Clauses and Schedules – Implementation Plan.
- 3.2.4. The Supplier shall produce a Remediation Report detailing any remediation required in the Buyer's current [REDACTED] platform to achieve the agreed design.
- 3.2.4.1. The Supplier shall provide a full set of Architectural Artefacts to include, as a minimum, a context model, component model (high level design), service design, deployment model (low level design), test design, test plan and a delivery plan.
- 3.2.4.2. The test design shall include the following, as a minimum, for each in scope platform: -
- a) Testing against vendor reference architecture.
 - b) Testing of failover capabilities.
 - c) Testing of integration with Buyer processes and provisioning systems.
 - d) Tests for the templates defined as part of the design.
 - e) Testing of Workload migration.
 - f) Testing of documented connectivity and location.
 - g) Testing all backup and recovery functions with Buyer's backup product.

- 3.2.4.3. The Supplier shall engage with the Buyer's Quality Assurance and Test team to ensure alignment with Buyer testing policies.
- 3.2.5. The Supplier shall provide a report which details both the capacity of the MVP platforms and the utilisation of their capacity by the discovered Workloads and any available capacity remaining in the respective platforms.
- 3.2.5.1. The Supplier shall provide that the design includes, at a minimum, 20% Surplus Capacity. This Surplus Capacity should be capable of supporting Workloads immediately without any action by the Parties.
- 3.2.5.2. The Supplier shall provide that the design includes at a minimum, 10% Burst Capacity over and above the Surplus Capacity. This Burst Capacity should be capable of supporting Workloads within 24 hours from the Buyer request to make it available as platform capacity.
- 3.2.6. The Supplier shall detail in the design where functions are only available with one of the two required platforms.
- 3.2.7. The Supplier shall detail in the design where functions may be enabled by additional procurement by the Buyer.
- 3.2.8. The design of the Private IaaS Platform will reference the Buyer [REDACTED] platform that was the subject of the discovery but must ensure that the Private IaaS Platform design is entirely separate with no reliance on the reference platform.
- 3.2.9. The design of the Private IaaS Platform must include a Performance Baseline of the Buyer [REDACTED] platform against both of the Supplier provided platforms with a reference set of Workloads to be agreed with the Buyer.
- 3.2.10. The Supplier shall ensure that the migration of Workloads to and from the new Private IaaS Platform has been verified by performing tests against test workloads created during the implementation phase, those workloads being part of the agreed design of Private IaaS Platform.
- 3.2.11. The Supplier shall ensure that the design includes options for Scaling up or down the provided platforms that comprise the Private IaaS Platform in cost-effective modular Upgrade (Scale Units) which can be implemented quickly to meet incoming demand.
- 3.2.12. The Supplier shall ensure the design details the available functions in relation to: -
- Billing (Showback/Chargeback)

- Capacity management
- Hyperscale provider portals (e.g. [REDACTED] integration to [REDACTED])
- Multiple environment types (production, pre-production)
- Multi-tenancy and network micro-segmentation
- Automation

- 3.2.13. The Supplier shall ensure that the design details the initial physical footprint and connectivity requirements (it can be assumed in relation to [REDACTED] that a connected model deployment will be required).
- 3.2.14. The Supplier shall ensure that the design encompasses the Greening Government intentions of the Buyer, which is part of the ICT and Digital Services strategy (<https://www.gov.uk/government/publications/greening-government-ict-and-digital-services-strategy-2020-2025/greening-government-ict-and-digital-services-strategy-2020-2025>) and shall ensure that the design states as a minimum, the power requirements at both maximum power saving settings and at maximum performance settings. The Buyer will require that the stated power requirements are met via a Service Level Performance Measure.
- 3.2.15. The Supplier shall ensure that the design details the Scale Unit sizes for the Private IaaS Platform.
- 3.2.16. The Supplier shall ensure that the design details which of the technologies in the Private IaaS Platform will offer a Product Catalogue.
- 3.2.17. The Supplier shall ensure that the design details the template creation process for items in the Product Catalogue and how these templates are to be consumed.
- 3.2.18. The Supplier shall ensure that the design details the physical resilience in each of HODC1 and HODC2.
- 3.2.19. The Supplier shall ensure that the design details how the Service Levels are to be achieved in each datacentre both in normal operation and in the event of the loss of a single datacentre.
- 3.2.20. The Supplier shall ensure that the design details how the Private IaaS Platform shall be integrated into the Buyer's existing Service Management (ITOC) and Security (CSOC) tooling and processes.

- 3.2.21. The Supplier shall ensure that the design provides a fully populated Break-Fix RACI itemising the technical services and the support framework requirements in scope for agreement with the Buyer. The RACI shall specify where there is a requirement for the Buyer to participate in any service activity that is underwritten by the Service Levels.
- 3.2.22. The Supplier shall be responsible for maintaining this RACI.
- 3.2.23. The Supplier will use the RACI as part of their obligations specified in section 2.1.3.2 to effectively manage those elements of the RACI where responsibility lies with the Buyer or Buyer Hosting Capability Supplier through the creation and maintenance of an acceptable Operational Level Agreement (OLA).

4. IMPLEMENTATION, TESTING AND ACCEPTANCE OF LIVE SERVICE

4.1. Implementation

- 4.1.1. The Supplier shall procure all required hardware, software and accessories required for the Achievement of Implementation Milestone Imp-M1: Procurement and Delivery to be completed as per the agreed design.
- 4.1.2. The Supplier shall work with the Buyer's teams to verify the reservation or allocation of physical data centre space and power, smart hands support and network connectivity required for the implementation to be completed as per the agreed design. The Supplier shall ensure that all Supplier Personnel comply with Buyer Access Policies at all times.
- 4.1.3. The Supplier shall allocate personnel for the implementation to be completed as per the agreed design and timescales.
- 4.1.4. The Supplier shall document the changes required for hardware installation and seek agreement via Technical Change control.
- 4.1.5. The Supplier shall liaise with the Buyer Data Centre teams to arrange for delivery of hardware to HODC1 and HODC2.
- 4.1.6. The Supplier shall deliver the required hardware and associated accessories to HODC1 and HODC2.
- 4.1.7. The Supplier shall perform the physical installation in both HODC1 and HODC2.
- 4.1.8. The Supplier shall agree successful hardware installation with the Buyer.
- 4.1.9. The Supplier shall document the changes required for hardware configuration and seek agreement via Technical Change control.
- 4.1.10. The Supplier shall implement the agreed hardware configuration.
- 4.1.11. The Supplier shall agree successful hardware configuration with the Buyer.
- 4.1.12. The Supplier shall document the changes required for [REDACTED] configuration and seek agreement via Technical Change control.
- 4.1.13. The Supplier shall document the changes required for remediation of the Buyer [REDACTED] configuration and seek agreement via Technical Change control.
- 4.1.14. The Supplier shall implement the agreed configurations.
- 4.1.15. The Supplier shall agree successful configuration with the Buyer.

- 4.1.16. The Supplier shall create templates for virtual machines and product catalogue services agreed prior to the Achievement of Design Milestone Design-M2 – Discovery and Architecture.
- 4.1.17. The Supplier shall document the changes required for monitoring / management integration configuration and seek agreement via Technical Change control.
- 4.1.18. The Supplier shall implement the agreed monitoring / management configuration.
- 4.1.19. The Supplier shall agree successful monitoring / management configuration with the Buyer.
- 4.1.20. The Supplier shall document the changes required for the backup configuration and seek agreement via Technical Change control.
- 4.1.21. The Supplier shall implement the agreed backup configuration.
- 4.1.22. The Supplier shall agree successful backup configuration with the Buyer.
- 4.1.23. The Supplier shall provide an “as installed” document which records how the Private IaaS Platform was implemented and how it correlates to the agreed design and details any variance from the agreed design.
- 4.1.24. The Supplier shall seek acceptance of the completed Detailed Implementation Plan in line with the process defined in Framework Schedule 4, Annex 3, Schedule S1 – Additional Clauses and Schedules – Implementation Plan. .
- 4.1.25. The table below shows Implementation stages and Milestones applicable to the implementation of the Private IaaS Platform.

4.2. Testing

- 4.2.1. The Supplier shall complete vendor compliance tests to ensure alignment to the reference architecture design.
- 4.2.2. The Supplier shall test all (including cross DC) failover capabilities of the Private IaaS Platform to demonstrate compatibility with meeting SLA requirements.
- 4.2.3. The Supplier shall ensure compatibility and integration with existing processes for Showback/Chargeback data, capacity, monitoring and Alerting.
- 4.2.4. The Supplier shall ensure compatibility and integration with existing Cloud Providers provisioning systems.
- 4.2.5. The Supplier shall deploy templates for Workload testing.
- 4.2.6. The Supplier shall create sample test Workloads from the templates.

- 4.2.7. The Supplier shall migrate sample Workloads from Buyer [REDACTED] to new Private IaaS Platform [REDACTED]
- 4.2.8. The Supplier shall migrate / transform sample Workloads from Buyer [REDACTED] to Private IaaS Platform [REDACTED]
- 4.2.9. The Supplier shall deploy sample services to Product Catalogue(s).
- 4.2.10. The Supplier shall test sample services deployed from Product Catalogue(s).
- 4.2.11. The Supplier shall test backup and restore functions of the Private IaaS Platform.
- 4.2.12. The Supplier shall test backup and restore of sample Workloads.
- 4.2.13. The Supplier shall test backup and restore of sample Product Catalogue service.
- 4.2.14. The Supplier shall produce a Performance Baseline report for the Buyer's acceptance based on the data from the test Workload operations. The requirements for this report are detailed in section 6.2.6.
- 4.2.15. The table in section 4.4 shows Implementation stages and Milestones applicable to the implementation of the Private IaaS Platform.

4.3. **Acceptance of Live Service**

- 4.3.1. For the Supplier to Achieve Acceptance Milestone ImpAcc-M1: Acceptance of Live Service , the Supplier will have Achieved all other milestones.
- 4.3.2. The Supplier shall provide evidence for the Achievement of Acceptance Milestone ImpAcc-M1: Acceptance of Live Service to demonstrate: -
- Documentation of the provided Service.
 - Asset details of all infrastructure for inclusion in the Buyer CMDB.
 - Licence details for all components.
 - Test results from Test Plan.
 - Agreed OLA with Buyer's Hosting Capability Provider as per the requirements in section 3.2.23.
 - Sample of operational reports (to include Alert, Event, capacity and billing reports).
 - Sample Service Report on Service Level measures.

4.3.3. The Supplier shall perform handover to the Buyer's Hosting Capability Provider as part of the Deliverables to Achieve Acceptance of Milestone ImpAcc-M1: Acceptance of Live.

4.3.3.1. The handover will include at a minimum: -

- The Architectural Artefacts for the agreed design
- An OLA agreed by the Buyer and the Buyers Hosting Capability Provider
- Documentation of the Private IaaS Platform, included template creation, usage and maintenance
- Licence details for all components
- Performance Baseline Report
- Asset details of all infrastructure supplied

4.3.4. Service Periods commence at Achievement of Acceptance Milestone ImpAcc-M1.

4.4. Delivery Milestones

Design Milestone Design-M1 – Security Clearance and Connectivity	
Deliverables	<ul style="list-style-type: none">• Week 1: Submit all Supplier Cleared Resources requests/transfer requests for entire Supplier Personnel team where required.• Week 1: Identify and request any physical infrastructure (e.g. floor space, power and networking requirements in the HODCs.)
Design Milestone Design-M2 – Discovery and Architecture	
Deliverables	<ul style="list-style-type: none">• Achievement of Design Milestone Design-M1• Discovery Report (section 3.2.3)• Remediation Report (section 3.2.4)• MVP and Capacity Report (section 3.2.5)• Supplier Software and Supplier Background IPRs (Call Off Terms Clause 21.4.2)• Architectural Artefacts (section 2.5.2.3) to include:<ul style="list-style-type: none">• Context Model• Component Model (High Level Design)• Deployment Model (Low Level Design)• Test Strategy• Test Plan

	<ul style="list-style-type: none"> • Within 20 Working Days of the Commencement Date, provide: <ul style="list-style-type: none"> - • Bespoke Information Security Management System (section 6.4.6.3 and Call Off Terms Schedule S3 (Security Requirements), Part B (Long Form Security Requirements)) • Security Management Plan (section 6.4.6.3 Call Off Terms Schedule S3 (Security Requirements), Part B (Long Form Security Requirements)) • Within 30 Working Days of the Commencement Date, provide: <ul style="list-style-type: none"> - • Detailed Implementation Plan (section 3.2.3.1) • BCDR Plan (section 6.3.3.3 and Call Off Terms Clause Schedule S6 Business Continuity and Disaster Recovery) • Break-Fix RACI (section 6.4.6.2) • Patch Management Plan also known as Maintenance Schedule (section 6.4.6.2 and Call Off Terms Clause 14.4)
Milestone Date	
Time of the essence? (Y or N)	Y (Y or N)
Buyer responsibilities	<ul style="list-style-type: none"> • None
Milestone Payments	
Delay Payments	
Implementation Milestone Imp-M1: Procurement and Delivery	
Deliverables	<ul style="list-style-type: none"> • Achievement of Design Milestone Design-M2 • Hardware and Software ordered (section 4.1.1) • Reservation of HODC1 and HODC2 Physical Space and Power (section 4.1.2) • Defined Technical Change for Network requirements (section 4.1.2) • Defined Resource Plan (section 4.1.3) <p>Required Hardware and Software delivered to HODC1 and HODC2 (section 4.1.6)</p>
Milestone Date	

Time of the essence? (Y or N)	Y
Buyer responsibilities	None
Milestone Payments	████████
Delay Payments	████
Implementation Milestone Imp-M2: Install and Configure	
Deliverables	<ul style="list-style-type: none"> • Achievement of Implementation Milestone Imp-M1 • Private IaaS Platform Physical Install (section 4.1.8) • Private IaaS Platform Hardware Configuration (section 4.1.11) • Private IaaS Platform Configuration (section 4.1.15) • Private IaaS Platform Monitoring Configuration (section 4.1.19) • Private IaaS Platform Backup Configuration (section 4.1.22) • Provide an “as-installed” document detailing implementation in relation to design (section 4.1.23)
Milestone Date	████████
Time of the essence? (Y or N)	Y
Buyer responsibilities	None
Milestone Payments	████████
Delay Payments	████
Testing Milestone ImpTest-M1: Design Baseline Conformance	
Deliverables	<ul style="list-style-type: none"> • Vendor Compliance Confirmation (section 4.2.1) • Failover and Resilience Confirmation (section 4.2.2) Integration with existing toolsets and processes (section 4.2.3 / 4.2.4)
Milestone Date	████████
Time of the essence? (Y or N)	Y

Buyer responsibilities	None
Milestone Payments	██████████
Delay Payments	██████
Testing Milestone ImpTest-M2: Template Creation and Deployment	
Deliverables	<ul style="list-style-type: none"> • Achievement of Testing Milestone ImpTest-M1 • Templates Deployed (section 4.2.5) • Test Workloads Created (section 4.2.6) • Product Catalogue sample services Created (section 4.2.9) • Workload Migration Testing Complete (section 4.2.7 / 4.2.8) • Service Testing Complete (section 4.2.10) • Backup Testing Complete (section 4.2.12 / 4.2.13) Performance Baseline Report (section 4.2.14)
Milestone Date	██████████
Time of the essence? (Y or N)	Y
Buyer responsibilities	None
Milestone Payments	██████████
Delay Payments	██████
Acceptance Milestone ImpAcc-M1: Acceptance of Live Service	
Deliverables	<ul style="list-style-type: none"> • Achievement of Testing Milestone ImpTest-M2 • Delivery of artefacts (section 4.3.2) • Successful handover to Hosting Capability Supplier (section 4.3.3)
Milestone Date	██████████
Time of the essence? (Y or N)	Y
Buyer responsibilities	None

Milestone Payments	
Delay Payments	

Table 2 - Delivery Milestones

5. ONGOING MAINTENANCE, EXPANSION AND UPGRADE

5.1. Ongoing Maintenance

- 5.1.1. The Supplier shall provide Service Support of the Private IaaS Platform including hardware break/fix and software support.
 - 5.1.1.1. The Supplier shall replace any failed hardware component of the Private IaaS Platform within 4 hours of the failure occurring as per SL9.
 - 5.1.1.2. Any data bearing component of the Private IaaS Platform will be maintained by the Buyer.
- 5.1.2. The Supplier shall provide 24/7 operational support for the Private IaaS Platform to a 99.99% Availability Service Level.
- 5.1.3. The Supplier shall use the Buyer's existing Problem & Incident Management Processes and tooling in their support and maintenance role.
- 5.1.4. The Supplier shall use the Buyer's existing Technical Change Management processes and tooling in their support and maintenance role.
- 5.1.5. The Supplier shall take ownership of all Changes, Problems and Incidents that relate to in-scope Private IaaS Platform Components.
- 5.1.6. The Supplier shall carry out the following support work:
 - Operational – 24/7 operational support for the Private IaaS Platform.
 - Service Management – 24/7 service support to manage and maintain the live Private IaaS Platform.
 - Performance – maintain all Service Levels.
 - Security – advise and offer mitigation for all cyber and data security concerns.
 - Monitoring and reporting.
 - Maintenance of all hardware and software licence validity.
 - Maintenance of all support contracts.
 - Produce Service Reports on Service Levels every month.
 - Produce Capacity Report every month.

- 5.1.7. The Supplier shall adhere to the most recent published versions of all Buyer policies and processes specified in the Contract, including those within Annex 5 of this document. Copies of these policies can be found in the Data Library section.
- 5.1.8. The Supplier shall ensure that all repaired or replacement parts are handled in line with the Buyer policies on media destruction.
- 5.1.9. Shared service support (Buyer, Supplier and Buyer's Third Parties)
 - 5.1.9.1. The Supplier will have a general reliance on the Buyer Networks and Infrastructure (N&I) team to grant the relevant access rights to network and compute components.
 - 5.1.9.2. The Supplier shall engage with both Buyer and Buyer's Third Party teams in relation to their Service Support responsibilities.
- 5.1.10. Out of scope for Supplier service support
 - 5.1.10.1. The Buyer and Buyer's Third Parties are responsible for support of all infrastructure which is not part of the contracted Service.
- 5.1.11. Hardware and software licencing
 - 5.1.11.1. The Supplier is responsible for provisioning hardware and software licencing for all in-scope services.
 - 5.1.11.2. The Supplier is responsible for maintaining up to date Third Party Software licensing and is responsible for reporting consumption and volumes of the licencing against asset lists and advising when renewal is required. The Supplier shall provide any information it has in relation to any licencing model which could provide reduced cost to the Buyer.
- 5.1.12. Virtual server management
 - 5.1.12.1. The Supplier shall Monitor the Private IaaS Platform as per the requirements detailed in section 6.
 - 5.1.12.2. The Supplier is not responsible for Monitoring the components of the individual VMs such as, OS and application layers.
- 5.1.13. Asset Management
- 5.1.14. The Supplier shall align to the Buyer "Service Asset & Configuration Management Operating Model" policy for Security Asset Configuration Management (SACM).

- 5.1.15. The Supplier shall contribute to the current Configuration Management Database (CMDB) / [REDACTED] used for all service components that are in scope for [REDACTED] domain and either provide a copy of amendments to Service Management and Asset & Config Team or maintain in the Buyer's Service Management Tooling. The CMDB/[REDACTED] is audited monthly, the Supplier shall ensure asset information and Configuration Item data is up to date.
- 5.1.16. The Supplier shall actively identify and inform the Buyer about redundant Assets (hardware and software) to support cost reduction on a calendar quarterly basis.
- 5.1.17. The Supplier shall ensure all hardware and software remains on supported versions.
- 5.1.18. Knowledge Base
- 5.1.18.1. The Supplier shall align with Buyer "Knowledge Management Operating Model" policy including writing and updating knowledge articles in [REDACTED] [REDACTED] and [REDACTED]
- 5.1.18.2. Information provided to comply with section 5.1.18.1 shall include, but not be limited to:
- Knowledge articles on all support and maintenance of the Service.
 - Knowledge articles to aid the correct routing of Service Incidents.
 - Knowledge articles to assist with the Shift-Left of Service Incidents resolutions by other support teams.
 - OLAs required to run and integrate the service.
 - CI Support Documents, Operational Manuals and Playbooks describing the end to end managed service operations, interactions and handoffs between suppliers.
- 5.1.18.3. The Supplier shall support the Buyer in writing and updating architectural, design and service documentation.

5.2. Expansion

- 5.2.1. The Supplier will use the Capacity Model to identify and work with the Buyer to successfully manage future expansion of the Private IaaS Platform based on trends of capacity usage and Demand Management.

- 5.2.2. The Supplier shall in all cases provide modular expansion which does not impact any existing capacity and can be deployed without impacting service provision. Any expansion should be additive and not require expenditure on any existing Private IaaS Platform component.
- 5.2.3. Any expansion options shall be based solely on the Scale Units and associated costs, irrespective of equipment revision by the Supplier.
- 5.2.4. Updates to the Scale Units available may occur during the Contract. The Buyer will be solely responsible for accepting amendments to the definitions or capacity of the agreed Scale Units.
- 5.2.5. For any agreed expansion, the Supplier shall provide a fully revised set of Architectural Artefacts, a delivery, implementation, test and acceptance plan for further Buyer approval. Sections 4.1 and 4.2 provide the detailed implementation and test requirements for any expansion.
 - 5.2.5.1. The Supplier shall, at the conclusion of any successful expansion, provide an updated “as installed” document to the Buyer.
 - 5.2.5.2. The Supplier shall ensure that the implementation of the agreed expansion is performed within 28 days from agreement.
- 5.2.6. The Supplier shall ensure that the Buyer has the option to acquire Scale Unit hardware at contract exit to maintain platform integrity. The price for the acquisition of any supplied Scale Units shall be commensurate with the prices provided for the acquisition of the MVP hardware infrastructure (section 2.8.3).

5.3. Upgrades

- 5.3.1. For any agreed Upgrade, the Supplier shall provide a fully revised set of Architectural Artefacts, a delivery, implementation, test and acceptance plan for further Buyer approval. Please refer to section 3.2 for the detailed design requirements for any Upgrade.
- 5.3.2. The Supplier shall provide details of new feature and capability releases to the Buyer as releases occur. These details, along with Supplier confirmation of their readiness to install the Upgrade, should be provided within 28 days of the Upgrades release by the respective technology provider.
- 5.3.3. The Buyer will be solely responsible to decide if a release is to be installed.

- 5.3.4. The Supplier shall, at the conclusion of any successful Upgrade, provide an updated “as installed” document to the Buyer.
- 5.3.5. The Supplier shall impact assess any applicable Upgrades.
- 5.3.6. The Supplier impact assessment shall indicate what aspects or features of the service are impacted by the Upgrade and provide details of such impacts. The impact assessment should detail if the Upgrade is mandatory and also any changes to the licence or other associated costs.
- 5.3.7. The Buyer shall solely decide if an Upgrade is to be applied.

6. SERVICE MANAGEMENT

- 6.1.1. Support team responsibilities
 - 6.1.1.1. The Supplier’s service management support organisation should align to the Buyer and Buyer’s Third Party support organisations.
 - 6.1.1.2. The Supplier shall provide the Private IaaS Platform “as a service” and deliver the Private IaaS Platform in a manner that can be managed securely and flexibly, operating using the public cloud paradigm.
 - 6.1.1.3. The Service Management toolset, performance reports and alignment of any Private IaaS Platform delivery with ITIL best practice for service management is central to the Service Management model.
 - 6.1.1.4. The Supplier’s Service Management operations and support services provided to the Buyer shall align with current ITIL best practice standards.
 - 6.1.1.5. At all times throughout the Contract Period, the Supplier maintain a current ISO 27001 certification.
 - 6.1.1.6. The Supplier shall ensure that the Supplier Personnel have the pre-requisite qualifications and experience to deliver the Services and the Buyer expects to be able to see valid certifications and experience on request for Supplier Personnel.
 - 6.1.1.7. Service Incidents must be raised “on-tool” via Buyer’s Service Management tool and will not be raised to the Supplier by phone or email except in the following circumstances:

- Strategic Service Desk (SSD) to follow up on open Service Incidents and requests.
- Service Management for service escalations and call out of the Duty Manager.

6.1.1.8. The Supplier shall run a shift pattern to ensure 24x7 coverage.

6.1.1.9. The Supplier shall support Problem and Change management activities as required.

6.1.2. Service Incidents, Problems, Changes and Releases

6.1.2.1. The Supplier shall be responsible for Resolving all Service Incidents, Problems, Technical Changes and Release for the Private IaaS Platform.

6.1.2.2. The Supplier shall comply with the relevant Buyer policies in Annex 5.

6.1.2.3. Without exception, all Service Incidents, Problems, Changes and Releases within the environments under the Service Levels must be recorded on Buyer's Service Management tool using the processes defined in the Buyer's Operating Models – Annex 5.

6.1.2.4. The required Service Incidents resolution times are set out at the Service Level table in Annex 1.

6.1.3. Capacity Management

6.1.3.1. The Supplier shall produce and maintain a Capacity Model for the Service which is shared with the Buyer at monthly service management reviews.

6.1.3.2. The Supplier shall ensure adequate planning and expansion of the capacity is implemented so that the Private IaaS Platform does not suffer from lack of capacity.

6.1.3.3. The Capacity Model shall include the following information, but not limited to:

- Capacity Requirements required to support the current Workloads.
- Details of any capacity constraints that may require additional expansion.
- Details of any capacity constraints that may be impacting upon system performance.
- Details of any capacity constraints that may impact upon system stability and Availability.
- Potential capacity improvements.

- Report of capacity underutilisation.
- 6.1.3.4. The Supplier shall work collaboratively with the Buyer and its Third Parties as nominated by the Buyer to provide the optimum amount of Private IaaS Platform capacity to meet business needs.
- 6.1.3.5. The Supplier shall ensure that capacity management is performed at appropriate thresholds as agreed with the Buyer to ensure that additional capacity can be deployed far enough in advance to avoid business disruption.

6.2. Performance requirements

6.2.1. Availability Service Level

6.2.1.1. The Service Level Performance Measure for the Availability Service Level shall always be a minimum of 99.99% for the entire Contract Period.

6.2.1.2. Availability Service Level shall be measured as a percentage of the total time in a Service Period, in accordance with the following formula:

$$\text{Availability \%} = (\text{MP} - \text{SD}) \times 100 : / (\text{divided by}) \text{MP}$$

where:

MP = total number of minutes, excluding Permitted Maintenance, within the relevant Service Period; and

SD = total number of minutes of Service Downtime

6.2.1.3. The Supplier shall provide measurements of Availability Service Level from the Achievement of Acceptance Milestone ImpAcc-M1.

6.2.2. Service Period Commencement

6.2.2.1. The first Service Period commences on the Achievement of Acceptance Milestone ImpAcc-M1. Service Credits are applicable from the commencement of the first Service Period.

6.2.3. Maintenance

6.2.3.1. The Supplier shall ensure compliance with all Buyer policies and procedures in respect to maintenance and Technical Change process.

6.2.3.2. Maintenance shall not, unless otherwise agreed by the Buyer, introduce any negative impact to Service performance or introduce any Service Downtime.

6.2.3.3. The Supplier shall ensure that all non-service impacting Changes required for ongoing maintenance to be standardised, pre-approved and automated wherever possible.

6.2.4. Resiliency

6.2.4.1. Where in-built resilience and redundancy of the Service enables the business application to continue without interruption, this will not be counted as Unavailability.

6.2.5. RTO, RPO, WRT and MTD

6.2.5.1. The Supplier shall implement an RPO and RTO. For physical hardware assets, the Supplier shall meet the baselines RPO and RTO.

6.2.5.2. The assets of the Private IaaS Platform are:

- Physical assets
 - Any hardware supplied under this Contract
- Virtualised Assets:
 - Any virtualised assets that form part of the Private IaaS Platform
- Infrastructure as Code:
 - Any deployed code from the Supplier

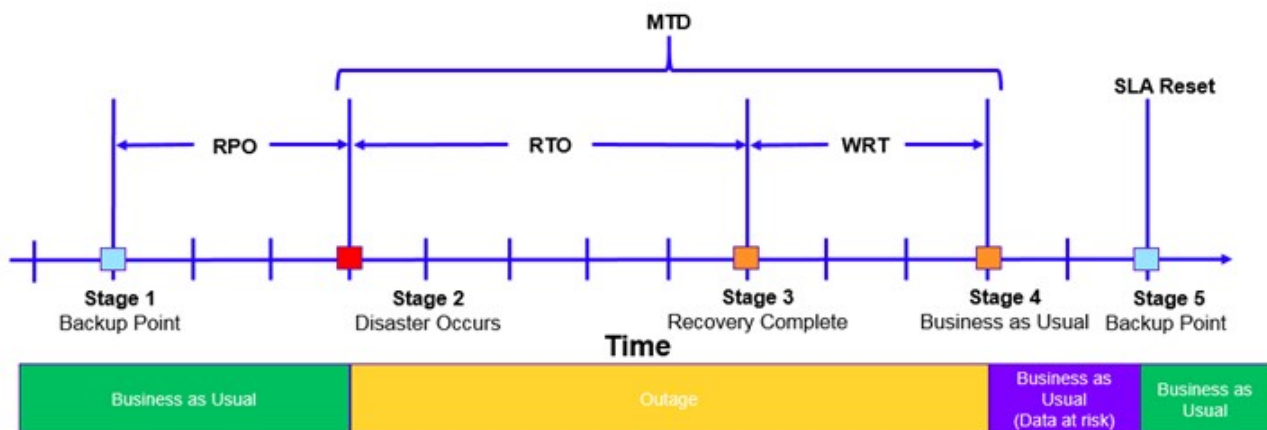


Figure 2 - RTO, RPO, WRT and MTD timeline

6.2.5.3. For physical assets:

- RTO (Recovery Time Objective) is 4 hours
- The RPO (Recovery Point Objective) is last known good configuration change or every 24 hours, whichever is most recent
- The WRT (Work Recovery Time) is 4 hours
- The MTD (Maximum Tolerable Downtime) is 8 hours

6.2.5.4. For virtualised assets:

- RTO (Recovery Time Objective) is 15 minutes
- The RPO (Recovery Point Objective) is last known good configuration change or every 15 minutes, whichever is most recent
- The WRT (Work Recovery Time) is 4 hours
- The MTD (Maximum Tolerable Downtime) is 4 hours 15 minutes

6.2.5.5. For infrastructure as code:

- RTO (Recovery Time Objective) is last known good commit/write
- The RPO (Recovery Point Objective) is last known good commit/write
- The WRT (Work Recovery Time) is 4 hours
- The MTD (Maximum Tolerable Downtime) is 4 hours 15 minutes

6.2.5.6. Definitions of RPO, RTO, WRT and MTD

- Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time.
- Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online.
- Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity post the RTO for example, checking the databases and logs for consistency.
- Maximum Tolerable Downtime (MTD) is the sum of RTO and WRT which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences.

6.2.6. Hardware Performance Monitoring

- 6.2.6.1. The Supplier shall provide monthly Performance Monitoring Reports for the Buyer to review showing performance of all aspects of the Private IaaS Platform hardware infrastructure. These reports shall be provided in accordance with the Call Off Terms and shall show the performance of all hardware components in relation to vendor reference values and include relevant measures for the hardware for further analysis. The required contents of the Performance Monitoring Reports as set out in the Call Off Terms also apply.
- 6.2.6.2. The Supplier shall reference the Performance Baseline established during the design phase in section 3.2.9 in the monthly report to show compliance with the established baseline. The Supplier shall manage and resolve any issue which results in performance below the baseline.

6.3. Security requirements

6.3.1. Cyber security and CSOC

6.3.1.1. The Cyber Security Operations Centre (CSOC) is the Buyer's internal function which designs, controls and currently operates the Buyer's protective monitoring solution. The CSOC is contactable 24 x 7 x 365. There will be an Operational Level Agreement (OLA) between the Supplier and CSOC which will describe the interfaces between both organisations (to be agreed as part of the Security Management Plan required for the Achievement of Design Milestone Design-M2).

6.3.1.2. In scope for Supplier

- The Supplier shall ensure that all components of the Private IaaS Platform are being monitored for Security Events as agreed with the Buyer and its organisations (ITOC and CSOC).
- The Supplier shall develop Indicators of Compromise (IoC) and information from the IoC being delivered to the Buyer CSOC.
- The Supplier is responsible for the security and integrity of Supplier Personnel and shall perform several account management tasks and ad hoc, daily, weekly, monthly, quarterly and half-yearly security checks.
- The Supplier shall use the Buyer's continuous vulnerability scanning tools on the Private IaaS Platform using the latest available threat libraries.
- The Supplier shall provide a vulnerability scan report and remediation plan, at a minimum, every month. Should an immediate risk become apparent, the Supplier shall immediately notify the Buyer.
- If the event of termination or expiry of the Contract, the Supplier shall remove all the Buyer's security Event logs from the Supplier environment in accordance with the secure decommission and sanitisation guidelines set by Her Majesty's Government.

6.3.2. Access control

6.3.2.1. In accordance with the Buyer's Security Policy, the Supplier will maintain compliant end user and administrative access security policies and procedures in line with Buyer security policies. The Supplier shall perform monthly audit checks to ensure End User and Administrator access permissions for all accounts which access the Private IaaS Platform are correct and act on the results of these checks in a timely manner.

6.3.2.2. The Supplier shall provide notification and details of the audit check outcome to the Buyer without delay of any inaccuracy, variance or anomaly resulting from the audit check.

- 6.3.2.3. The Supplier shall share details of any audit check with the Buyer as part of the monthly reporting cycle.
- 6.3.2.4. Without delay, the Supplier shall provide to the Buyer's operational security function a record of access where End Users and Administrators are suspected of breaches of policy, inappropriate use of resources, or fraudulent use of data and access management.

6.3.3. Business Continuity

- 6.3.3.1. The Supplier shall comply with the relevant Buyer Business Continuity policies in Annex 5.
- 6.3.3.2. The Supplier shall provide their own business continuity plan related to their continued support in the event of the Supplier's locations becoming Unavailable.
- 6.3.3.3. The Business Continuity and Disaster Recovery (BCDR) Plan and processes shall be provided within one month of the Commencement Date. The scope shall include:
 - The Supplier BCDR Plan.
 - The Supplier BCDR communication plan.
 - A risk assessment which will be supported by an Incident management plan and Incident response structure.
 - A business impact analysis that identifies critical functions required to run the services and a risk assessment against the loss of those services.
 - A breakdown of personnel who are directly connected to the service and any support personnel.
- 6.3.3.4. The Supplier shall test the BCDR Plan on an annual basis, Resolve/Fix any issues identified and inform the Buyer of all risks, threats and findings.

6.4. Monitoring and Reporting requirements

6.4.1. General Monitoring requirements

- 6.4.1.1. The Buyer currently utilises a range of Monitoring and Alerting tooling. One of the key ambitions for the Buyer is to improve the scope, depth and visualisation of Monitoring and Alerting tooling.

6.4.1.2. The Supplier shall utilise the Buyer Monitoring and Alerting Tooling. However, the Supplier shall be responsible for defining the Monitoring and Alerting thresholds within the tooling.

6.4.1.3. The Supplier shall ensure that all events generated from the Monitoring and Alerting Tooling raise a Service Incident within the Buyer SIEM tooling.

6.4.2. Tooling capability and metrics

6.4.2.1. Existing Buyer Monitoring capabilities and metrics will be maintained until replaced as part of the development of Buyer Monitoring requirements. The Supplier will assist the Buyer in identifying gaps in Monitoring, suggesting improvements to the current Monitoring design and collaborating with the Buyer Product Engineering team on the future Monitoring design.

6.4.3. Reporting requirements

- 6.4.3.1. The Supplier shall monitor all Key Performance Indicators (KPIs) set out in Annex 2 and produce a detailed monthly performance report.
- 6.4.3.2. The monthly Performance Monitoring Report should cover reporting data from the first day to the last day of each Service Period and should contain the following type of content:
 - Executive Summary
 - Performance of the Private IaaS Platform against all Service Levels and KPIs
 - Problem Management including root cause statement in the event of a P1 Service Incident within 3 working days and a corrective action plan to mitigate future occurrence
 - Change Management
 - Financial Statement
 - Risks and mitigations
 - Issues
 - Dependencies
 - List of single points of failure
 - Hardware performance (section 6.2.6)
 - Other reports on request

6.4.4. Meetings

- 6.4.4.1. The Supplier shall participate in monthly service reviews and any other meetings requested by the Buyer. Non-exhaustive examples are the Technical Change Board and Operational Board.
- 6.4.4.2. The Supplier shall represent the Private IaaS Platform by attending all meetings and forums arranged by the Buyer to ensure any plans, actions or requests presented during such meetings take into consideration the impact of decisions made covering technology, resources, costs, tools, processes, policies, assets, other Third Parties or locations.

6.4.5. Governance

- 6.4.5.1. In addition to the governance provisions set out in the Call Off Terms, the Supplier shall attend regular governance meetings as requested by the Buyer which affect the Private IaaS Platform to:

- Review Service Levels and Service Credits
- Address Service Incidents and Problems
- Analyse, review and approve Technical Changes
- Review risks and issues including mitigations
- Review and resolve any financial issues
- Provide advice, guidance and information on technical issues
- Review and Resolve/Fix any escalated issues from the Service Support and Engineering/Transformation teams
- Review service strategy and associated implementation approaches
- Review hardware and software licensing status

6.4.6. Documentation and Artefacts

6.4.6.1. The Supplier shall ensure that all documented artefacts describing the service model and its architecture are up to date, accurate and available to the Buyer throughout the Contract Period.

6.4.6.2. Notwithstanding any other provision of the Contract, the Supplier shall provide the following documentation within 30 Working Days of the Commencement Date:

- Detailed Implementation Plan (section 3.2.3.1)
- BCDR Plan
- Break-Fix RACI
- Patch Management Plan (Maintenance Schedule)

6.4.6.3. Notwithstanding any other provision of the Contract, the Supplier shall provide the following documentation within 20 Working Days of the Commencement Date:

- Security Management Plan
- Bespoke Information Security Management System

6.4.7. Risk and issue management

6.4.7.1. The Supplier shall follow the Buyer's Risk and Issue Management process for the management and classification of risks and issues, including:

- Identify risks for provision of the service
- Log all risks in the Risk Register
- Document actions, acceptance and mitigations
- Engage in the Buyer's risk management process

6.5. Buyer policies and procedures

- 6.5.1. The Supplier shall adhere to the principles and policies as defined in all Buyer and Government policies, processes and procedures listed in Annex 5.
- 6.5.2. Copies of policies and procedures listed in Annex 5 can be found in the Data Library. The documents listed in Annex 5 are for use in undertaking the obligations as set out in the Contract and must not be used for any other purpose.
- 6.5.3. The documents listed in Annex 5 may only be used within the scope of the current engagement with the Buyer. Except with the express prior written permission of the Buyer, these documents and the information contained herein may not be further published, disclosed, or used for any other purpose.

6.6. Testing requirements

- 6.6.1. The Supplier shall comply with the relevant Buyer Quality Assurance and Testing Strategy and Standards in Annex 5.

6.7. Training requirements

- 6.7.1. All on-boarded Supplier Personnel shall complete any mandatory Buyer training and compliance reviews.
- 6.7.2.

ANNEXES

1. ANNEX 1 - SERVICE LEVELS

1.1. Service Level Performance Measures

The Supplier shall meet the Service Level Measures detailed in Table 4 (Service Levels and Credits – Service Level Performance Measures) below, which shall be used in conjunction with section 1.2 to calculate Service Credits.

Overall Summary				
Category	Item 1	Item 2	Item 3	Item 4
Section A	Item A1	Item A2	Item A3	Item A4
	Item A1	Item A2	Item A3	Item A4
	Item A1	Item A2	Item A3	Item A4
	Item A1	Item A2	Item A3	Item A4
Section B	Item B1	Item B2	Item B3	Item B4
	Item B1	Item B2	Item B3	Item B4
	Item B1	Item B2	Item B3	Item B4
	Item B1	Item B2	Item B3	Item B4

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]		
[REDACTED]	[REDACTED]	[REDACTED]		
[REDACTED]	[REDACTED]	[REDACTED]		
[REDACTED]	[REDACTED]	[REDACTED]		
[REDACTED]	[REDACTED]	[REDACTED]		
[REDACTED]	[REDACTED]	[REDACTED]		

Table 3 – Service Levels and Credits – Service Level Performance

<p>[REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED]</p>	<p>[REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED]</p>
<p>[REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED]</p>	<p>[REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED]</p>
<p>[REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED]</p>	<p>[REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED]</p> <p>[REDACTED] [REDACTED] [REDACTED]</p>

1.2. Service Credits

1.2.1. Service Credits shall be calculated on the basis of Table 5 below.

<div style="background-color: black; width: 100%; height: 100%;"></div>	

Table 4 - Calculation of Service Credits

1.3. Critical Service Level Failure

1.3.1. A Critical Service Level Failure means a Service Level Failure for any of the following:

- a) Availability Service Level: where the Service is not Available for a consecutive period of one hour or greater in any rolling 12 consecutive Service Periods, or
- b) Availability Service Level: where the Service is not Available for less than one consecutive hour, more than once in any one Service Period, or
- c) Any three Service Levels from Service Levels SL4 to SL9 (inclusive) in any given Service Period, or
- d) Time to Fix Service Level: where the level of performance of the Supplier is less than 85% against the Measure of Service for any Priority level in any one Service Period, or
- e) Time to Fix Service Level: where the level of performance of the Supplier is less than an average of 90% against the Measure of Service for any Priority level in any rolling 12-month period.

1.3.2. Service Credit Cap is defined as follows:

For the period of the first 12 Service Periods (inclusive), 15% of the Contract Charges payable to the Supplier for the first 12 Service Periods (inclusive); and during the remainder of the Contract Period, 20% of the Contract Charges payable to the Supplier in the period of twelve (12) months immediately preceding the month in respect of which Service Credits are accrued.

2.

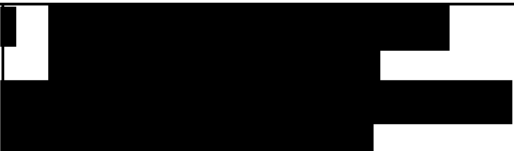
Black	Black	Black	Black	Black	Black	Black	Black	Black	Black	White	White	White	White	White	White
Black	Black	Black	Black	Black	Black	Black	Black	Black	Black	White	White	White	White	White	White
Black	Black	Black	Black	Black	Black	Black	Black	Black	Black	White	White	White	White	White	White
Black	Black	Black	Black	Black	Black	Black	Black	Black	Black	White	White	White	White	White	White

Table 6 - Key Performance Indicators (KPIs)

3. ANNEX 3 – DEFINED TERMS

Word	Acronym	Definition
Alert		<p>A warning that a threshold has been reached, something has changed, or a failure has occurred. Alerts are often created and managed by system management tools and are managed by the Event Management process.</p> <p>In the case of the Buyer's IT Service Management Tool, [REDACTED] Alerts are created from Raw Events based on pre-defined rules, Event mappings and Service mappings.</p>
Architectural Artefacts		<p>A set of documentation aligned to the Architectural governance of the Buyer. The documentation includes: -</p> <ul style="list-style-type: none"> Context Model Component Model Service Design Deployment model Detailed Implementation Plan
Architectural Discussion Forum	ADF	<p>Architectural advisory Boards for reviewing and recommending to the approving authority new and amended High-Level Designs. Peer review, advice and guidance to Technical Teams.</p>
As A Service	aaS	<p>A flexible commercial model with the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications</p>

Automated Alert		An Alert created automatically by monitoring or service management tooling in response to the breach of pre-configured thresholds or behaviours.
Automatic Transfer Switch		Automatic Transfer Switches (ATS) which can automatically switch power flow on redundant power infrastructures are essential wherever substantial power must be maintained. To ensure people's safety in a work or public space, or to maintain essential supplies to a vital process, the fast and efficient transfer of power is automatically managed by the ATS system.
Available and Availability		End Users accessing services hosted on the Private IaaS Platform are able to perform all agreed functions correctly, as set out in the Contract, and access and utilise all the functions of the services hosted on the Private IaaS Platform.
Break-Fix		The replacement of a failed component in an infrastructure item.
Burst Capacity		Additional unused infrastructure capacity which is physically installed but restricted from use due to Supplier configuration. Available to be deployed into live service upon Buyer request.
Change Management System	CMS	A system used to manage the lifecycle of ITSM change.
Cleared Resources		

		
Configuration Item	CI	Any component that needs to be managed in order to deliver an IT Service. Information about each CI, for example its Status, is recorded in a configuration record within the Configuration Management System and is maintained throughout its lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT Services, hardware, software, buildings, people, and formal documentation such as process documentation and Service Levels.
Configuration Management System	CMS	A set of tools and databases used to manage IT Service Configuration data. The CMS also includes information about Service Incidents, Problems, Known Errors, Changes and Releases and it may contain data about employees, suppliers, locations, Business Units, Buyers and Users. The CMS includes tools for collecting, storing, managing, updating and presenting data about all Configuration Items and their relationships. The CMS is maintained by Configuration Management and is used by all IT Service Management Processes.
Cyber Security Operations Centre	CSOC	The Buyer's Cyber Security Operations Centre which provides protective Monitoring for some elements of HODCx.
Data Centre		A secure facility designed to house computer systems and associated components, such as communication and storage.
DDaT	DDaT	Home Office Digital, Data and Technology.

End User		Any person authorised by the Buyer to use the IT Environment and/or the Services.
Enterprise Services	ES	The teams responsible for delivering common infrastructure services (not applications) that are consumed by multiple Buyer business Portfolios.
Event (General Definition)		<p>A change of state that has significance for the management of a Configuration Item or IT Service.</p> <p>The term Event is also used to mean an Alert or notification created by any IT service, Configuration Item or Monitoring tool. Events typically require IT Operations personnel to take actions and often lead to Service Incidents being logged.</p>
Event Management		The process responsible for managing Events throughout their lifecycle. Event Management is one of the main activities of IT Operations.
Event Management Plan (EMP)		The Event Management Plan (EMP) documents how Event Monitoring and management will be provided for a specific service or set of services. It is the agreement between the ITOC and the portfolio owning the service on the Event Monitoring and Management services to be provided by the ITOC.
Fault		A condition that causes a component to fail to perform its required function.
High Level Design / Component Model	HLD	<p>High Level Design – Process flowchart depicting each of the processes at a high level containing organisational swim lanes, process inputs & outputs, process phases and activities.</p> <p>Underpinning document containing process objectives, common principles and a matrix of responsibilities with responsibility narrative.</p>

HODC1	HODC1	Home Office Data Centre	
HODC2	HODC2	Home Office Data Centre	
HODCx	HODCx	A term used to represent Home Office Data Centres.	
Hosting Capability Provider		A Third Party to the Buyer who manages the core infrastructure provided in HODCx.	
Hyper Converged Infrastructure	HCI	Hyper-converged infrastructure (HCI) is a software-defined IT infrastructure that virtualizes all of the elements of conventional "hardware-defined" systems. HCI includes, at a minimum, virtualized computing (a hypervisor), software-defined storage, and virtualized networking (software-defined networking).	
Incident		Unplanned interruption to, or quality reduction of an IT Service.	
Information Technology Operations Centre	ITOC	The Buyer's Information Technology Operations Centre.	
Intelligent Client		Intelligent Client organisations are capable of specifying the requirements to external participants and managing delivery outcomes. Fundamental to this is the management of those relationships to maximise value.	
IT Service Management	ITSM	A set of processes to manage the implementation and operation of IT Services.	
Key Performance Indicators	KPIs	KPIs evaluate the success of the Supplier in accordance with measures set out at Annex 2.	
Level 4 Support		<p>The Supplier's team which shall be the initial point of engagement for Service Incidents assigned to the Supplier. Service Incidents must be raised on-tool via ServiceNow and will not be raised to the Supplier by phone or email except in the following circumstances:</p> <ul style="list-style-type: none"> • SSD to follow up on open Service Incidents and Service Requests • Service Management for service escalations and call out of the Duty Manager 	

Low Level Design / Deployment Model	LLD	Low Level Design- Process flowchart depicting each of the processes at a lower level containing organisational and role swim lanes and process phases and activities. Underpinning process description matrix spreadsheet containing process steps, activity, description, inputs, outputs, touch points and role-based RACI matrix.
Minimum Viable Product	MVP	The smallest operable platform which has sufficient capacity to maintain the Buyer Workloads identified at the required Service Availability.
Maintenance Change		An alteration in state or configuration of a controlled item within the Change Management System (CMS).
Monitor / Monitoring		Repeated observation of a Configuration Item, IT Service or process to detect Events and to ensure that the current status is known. Monitoring should also provide early sight of future problems through analysis of trends.
NIST	NIST	National Institute of Standards and Technology
Non-Available		In relation to the IT Environment or the Services, that the IT Environment or the Services are not Available.

Non-Disclosure Agreement	NDA	A Non-Disclosure Agreement is a legally binding contract that establishes a confidential relationship. The party or parties signing the agreement agree that sensitive information they may obtain will not be made accessible to any others. An NDA may also be referred to as a confidentiality agreement.
Notification		An automated communication sent from the Service Management systems via authorised channel such as email or SMS.
Operational Level Agreement	OLA	An OLA supports the Supplier's delivery of IT services to the Buyer. The OLA defines the goods and services to be provided and the responsibilities of both the parties.
Performance Baseline		Metrics related to the performance of representative Workloads as configured and running on the source environment. Used

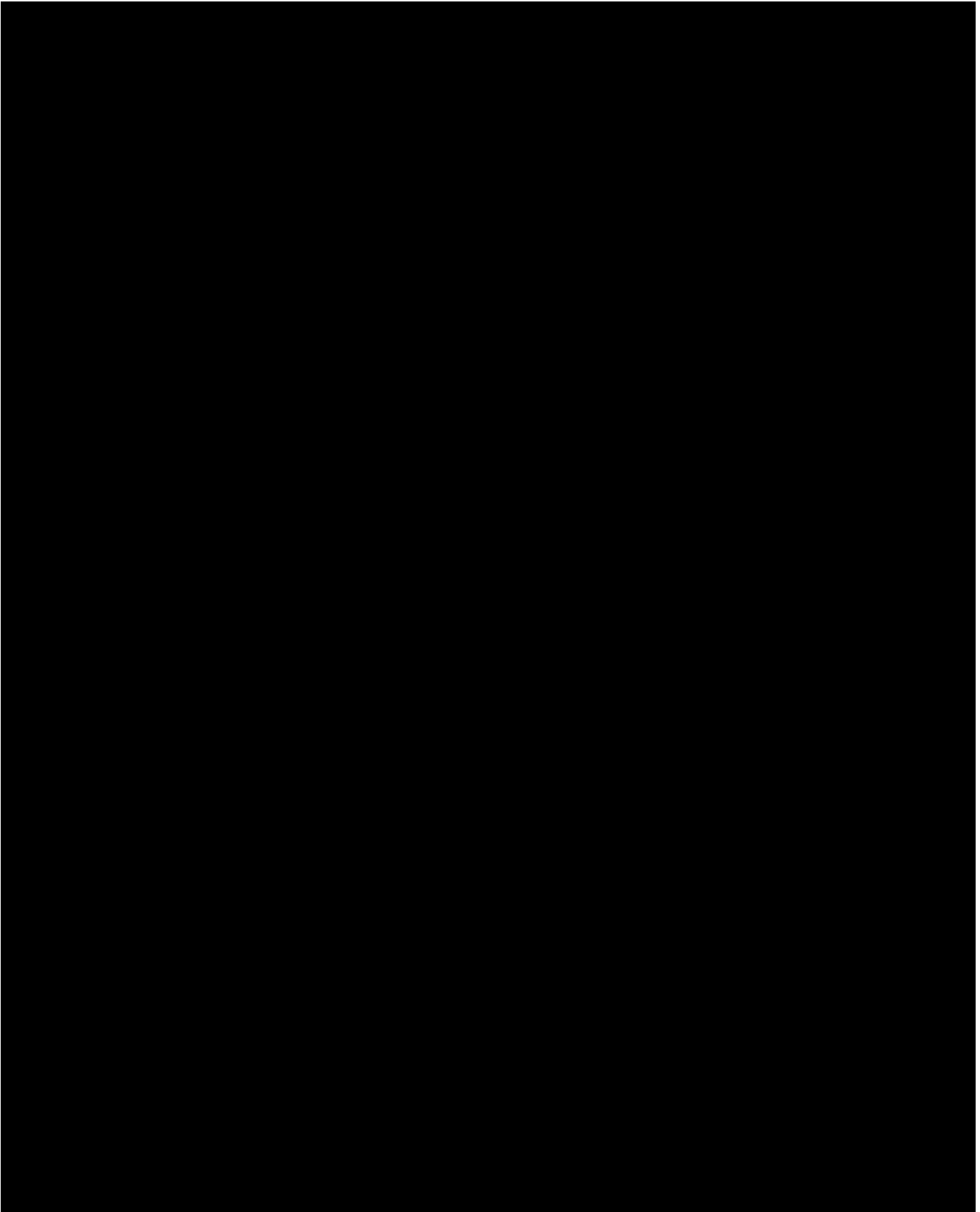
		as a measure of comparison for future performance metrics.
Permitted Maintenance		Maintenance which is determined, solely by the Buyer, as being excluded from the calculation of Availability Service Level.
Platform Level		The Private IaaS Platform HCI hardware and Supplier provided technologies, [REDACTED] and [REDACTED]
Priority 1 Service Incident	P1	when a Service is Unavailable to its users or where performance is so poor the service becomes unusable.
Priority 2 Service Incident	P2	When a Service is severely degraded to its users or there is a loss of resilience which, although not resulting in, significantly increases the risk of, a P1 Service Incident.
Priority 3 Service Incident	P3	A component failure that does not affect the performance or resilience of the Service.
Priority 4 Service Incident	P4	A Service Incident that is cosmetic in nature or has no or little effect on end-users.
Private IaaS Platform		The new [REDACTED] and [REDACTED] environments which comprise the in scope high level architecture
Problem		The cause of one or more Service Incidents.
Product Catalogue		A catalogue of consumable information technology related products and services available to customers.
RACI		A model used to help define roles and responsibilities. RACI stands for responsible, accountable, consulted and informed.
Recovery Point Objective	RPO	Determines the maximum acceptable amount of data loss measured in time.
Recovery Time Objective	RTO	Determines the maximum tolerable amount of time needed to bring all critical systems back online
Release		A set of authorised changes to a service or component.
Resolve/Fix/Resolution		When the Service is returned to a working state by rectifying the issue

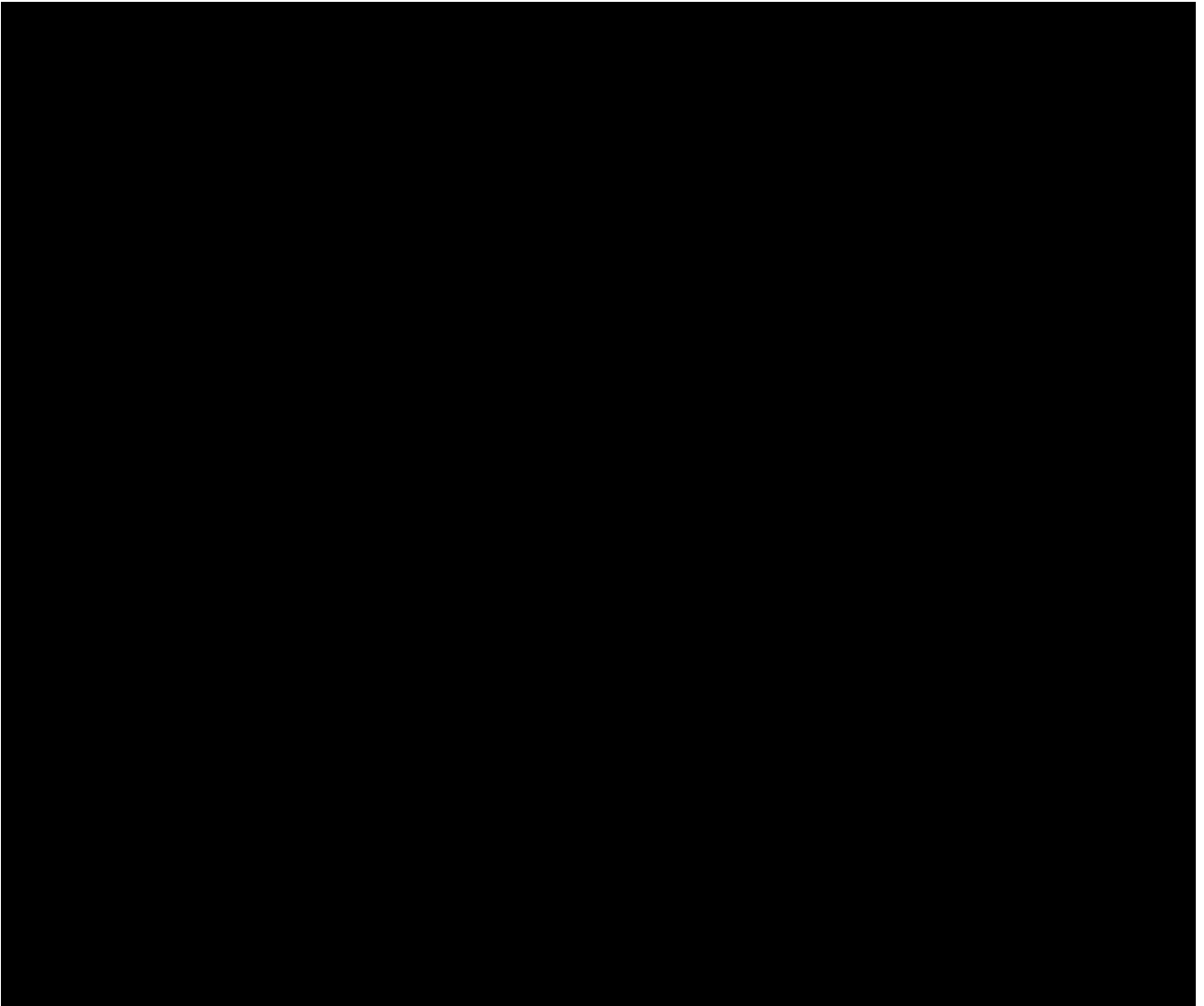
		<p>that resulted in a Service Incident, the state can be set as Resolved. If the user is satisfied with the resolution, the user can close the Service Incident, or the Service Incident is auto-closed after a certain time based on the Service Incident auto-close properties. Resolution means in relation to a Service Incident, either:</p> <ul style="list-style-type: none"> • The root cause of the Service Incident has been removed and the Services are being provided in accordance with the Services Description and Service Levels; or • The Buyer has been provided with a workaround in relation to the Service Incident deemed acceptable by the Buyer.
SACM	SACM	Service Asset and Configuration Management.
Scale / Scaling		<p>The addition or removal of infrastructure or software to increase or reduce the available capacity of the Private IaaS Platform. The limit of Scaling down shall be the MVP for the Private IaaS Platform which is required to maintain the required Service Level Availability.</p>
Scale Unit		<p>A defined configuration that can be added to the Private IaaS Platform. Both [REDACTED] and [REDACTED] will have its own Scale Unit defined.</p> <p>These defined Scale Units need to align to the 99.99% Availability requirement for the Service. Therefore, the minimum Scale Unit would include equal expansion in both datacentre instances.</p>
Service Availability		This is defined in section 6.2.1

Service Continuity Event		A Service Incident which the Buyer considers significant enough to raise as a disaster-level Event. Such an Event might limit Availability to multiple critical services.
Service Incident		An occurrence of a failure to deliver any part of the Services in accordance with the requirements, or the Performance Indicators, whether reported or not, that can disrupt or cause a loss of operations, services or functions.
Service Operating Hours		In relation to any Service, the hours for which that Service is to be operational.
Service Readiness Review	SRR	A standard governance process which determines whether the processes, documentation and skills are available to commence support for the live Service.
Service Request	SR	A request from a user for information, advice, a standard change, or access to a service.
Shift-Left		Moving the person, process, or technology closer to the Buyer and/or resolver team, resulting in a faster and more efficient and effective outcome. Implementing more self-service capabilities and deliver standardisation and repeatable solution patterns and Service Incident resolution through automation.
Strategic Service Desk	SSD	The Buyer's service desk to co-ordinate Service Providers and their services to achieve the end-to-end service levels needed to support Home Office's business functions.
Surplus Capacity		Additional unused infrastructure capacity which is physically installed and available for use.
Target Operating Model	TOM	A description of the desired state of the operating model of an organisation. When working on the operating model, it is normal to define the "as is" model and the "to be" model. The Target Operating Model is the "to be" model.

Technical Change		Technical Change is the process of requesting, planning, executing and evaluating changes to a system.
Technical Change Board		The Buyer's Board for the management of Technical Change. The two main goals of this Board are the prioritisation and approval for the process of Technical Change and to support traceability of change approval and implementation.
Technical Design Authority	TDA	The Buyer's Architectural Governance Boards for reviewing and approving authority for new and amended High-Level Designs. Peer review, advice and guidance to Technical Teams.
Total Cost of Ownership	TCO	A financial estimate intended to help buyers and owners determine the direct and indirect costs of a product or service. It is a management accounting concept that can be used in full cost accounting or even ecological economics where it includes social costs.
Unavailable/ Downtime		In relation to the Private IaaS Platform, that the Private IaaS Platform is not Available excluding any Permitted Maintenance.
Unplanned Maintenance		Maintenance carried out as a result of unexpected equipment failure.
Upgrade		The implementation of an increase in capability or an approved Release of software on the Private IaaS Platform.
Workload		A virtual machine or virtual appliance running on the Buyer [REDACTED] platform or new Private IaaS Platform.
Work Recovery Time	WRT	Determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity post the RTO for example, checking the databases and logs for consistency.

Table 7 – Defined Terms





5. ANNEX 5 - BUYER POLICIES

The Supplier shall follow and conform to all Buyer and HM Government policies, processes and procedures listed below (copies can be found in the Data Library):

5.1. Government policies

- The Government Digital Service Standards:
- <https://www.gov.uk/service-manual>
- The Government Digital Service Manual
- <https://www.gov.uk/service-manual>
- Government Digital Service Technology Code of Practice
- <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
- Government Digital Services Technology Code of Practice – Collection of Related Topics:
- <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice-related-guidance>
- Government Security Classifications
- <https://www.gov.uk/government/publications/government-security-classifications>
- General Data Protection Regulations
- <https://www.hm.gov.uk/government/publications/guide-to-the-general-data-protection-regulation>

5.2. Buyer Policies - Info security

- Information Assurance Policy

5.3. Buyer Policies - Operating models

- Cyber Security Incident Management Operating Model
- Enterprise Services Portal Operating Model
- Event Monitoring and Management Operating Model
- Incident Management Operating Model
- Problem Management Operating Model
- Release Assurance Operating Model
- Change Management Operating Model
- Knowledge Management Operating Model
- Service Asset & Configuration Management Operating Model
- External Software Asset Management Operating Model

- Risk and Issue Management Operating Model

5.4. **Buyer Policies - Business Continuity**

- Business Continuity Management policy and guidance
- Business Continuity quick guide
- Business Continuity top tips

5.5.



5.6. **Buyer Policies – Personnel security**

- Security Incidents Policy
- Government Response Level

5.7. **Buyer Policies - Cyber security**

5.7.1. Cyber security policies that apply from Commencement Date (can be found in Data Library)

- Firewall Policy
- Cyber Risk Management Policy
- Cyber Assurance Policy
- Password Policy
- Account Management Policy and Standard

5.8. **[Redacted] – Data Centres Site Security**

- [Redacted] security access requirements
- [Redacted] Site Conduct Guidance

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Attachment 2 – Charges and Invoicing

Details of the Charges payable by the Buyer to the Supplier (including any applicable Milestone Payments and/or discount(s), but excluding VAT) and payment terms/profile are specified below. All payments made to the Supplier shall be done so in accordance with the Payment Profile via BACS only. All Charges, pricing and invoicing are subject to the provisions of Call Off Terms Schedule 2 (Charges and Invoicing).

Charging Mechanisms

Pricing Model Reference	Charging Mechanism
Solution Delivery Milestones	<p><u>Milestone Payments</u></p> <p>Subject to the provisions of Paragraph 1.2 of Part C of Schedule 2 (Charges and Invoicing) to the Call Off Terms in relation to the deduction of Delay Payments, on the Achievement of a Milestone, the Supplier shall be entitled to invoice the Buyer for the Milestone Payment associated with that Milestone, less an amount equal to 10% of the applicable Milestone Payment (“Retention Amount”) which may be adjusted in line with the Milestone’s Incurred Costs.</p> <p>In the event the costs incurred by the Supplier relating to a Milestone (“Incurred Costs”) are lower than the corresponding Milestone Costs identified in the Pricing Model, the difference between the Incurred Costs and the Milestone Costs shall be shared equally between the Parties, by means of a credit (shown as a separate line) within the corresponding Supplier invoice, or by means of a separate credit note received by the Buyer no later than thirty (30) days of the corresponding invoice. The Supplier’s invoices for all Milestones shall detail the Incurred Costs, whether or not the Incurred Costs are lower than the Milestone Costs</p> <p><u>Retention Amounts</u></p> <p>On the Achievement of all Transition Milestones (Design-M1, Design-M2 , Imp-M1, Imp-M2, Test-M1, Test-M2, ImpAcc-M1), the Supplier shall be entitled to invoice the Buyer for an amount equal to the sum of all Transition Milestones Retention Amounts.</p>
Pay As You Go Pricing	<p><u>Service Charges</u></p> <p>Service Charges shall be invoiced by the Supplier for each Service Period in arrears in accordance with the requirements of Part D of Schedule 2 (Charges and Invoicing) of the Call Off Terms.</p> <p>If a Service Charge commences on a day other than the first day of a month; and/or ends on a day other than the last day of a month, the Service Charge for the relevant Service Period shall be pro-rated based on the proportion which the number of days in the month for which the Service is provided bears to the total number of days in that month.</p>

Pay As You Go Pricing – Additional Scale Units	<p><u>Service Charges</u></p> <p>Where the customer has requested additional Scale Units, the Supplier shall be entitled to invoice the Buyer with the increase in charges in accordance with the requirements of Part D of Schedule 2 (Charges and Invoicing) of the Call Off Terms.</p> <p>If a Service Charge commences on a day other than the first day of a month; and/or ends on a day other than the last day of a month, the Service Charge for the relevant Service Period shall be pro-rated based on the proportion which the number of days in the month for which the Service is provided bears to the total number of days in that month.</p>
Volume Term Commitment	<p><u>Upfront Payment</u></p> <p>Where the Buyer has requested an Upfront Volume Term Commitment, the Supplier shall be entitled to invoice the Buyer for the total requested number of Service Periods of the Volume Term Commitment, factoring in any discount factors, in accordance with the requirements of Part D of Schedule 2 (Charges and Invoicing) of the Call Off Terms.</p> <p><u>Service Charges</u></p> <p>Where the Buyer has requested the Volume Term Commitment to be invoiced monthly, the Service Charges shall be invoiced by the Supplier for each Service Period, in arrears, in accordance with the requirements of Part D of Schedule 2 (Charges and Invoicing) of the Call Off Terms.</p>

All invoices shall be submitted in accordance with Call Off Terms Part D to Schedule 2 (Charges and Invoicing).

For all Milestone Payments, the Supplier will be responsible to deliver the agreed scope within the agreed fixed price and will bear any risks or costs associated with delivery of the Services, including any potential delays.

Who and where to send invoices to:

Invoices will be sent via email as the primary method for delivery to the address below:



Invoice information required:

All invoices must include:

- A valid Purchase Order number.
- The contract reference number (C21669).
- The information called for at paragraph 1.2.3 of Part D to Schedule 2 (Charges and Invoicing).
- Where an invoice relates to a Milestone, the Supplier shall provide details of Incurred Costs.

Part A – Milestone Payments and Delay Payments

The Deliverables applicable for each Milestone are as set out at Appendix B: Specification and Requirements.

All Transition Milestone Payments are subject to the Retention Amounts as set out at Attachment 2 – Charges and Invoicing.

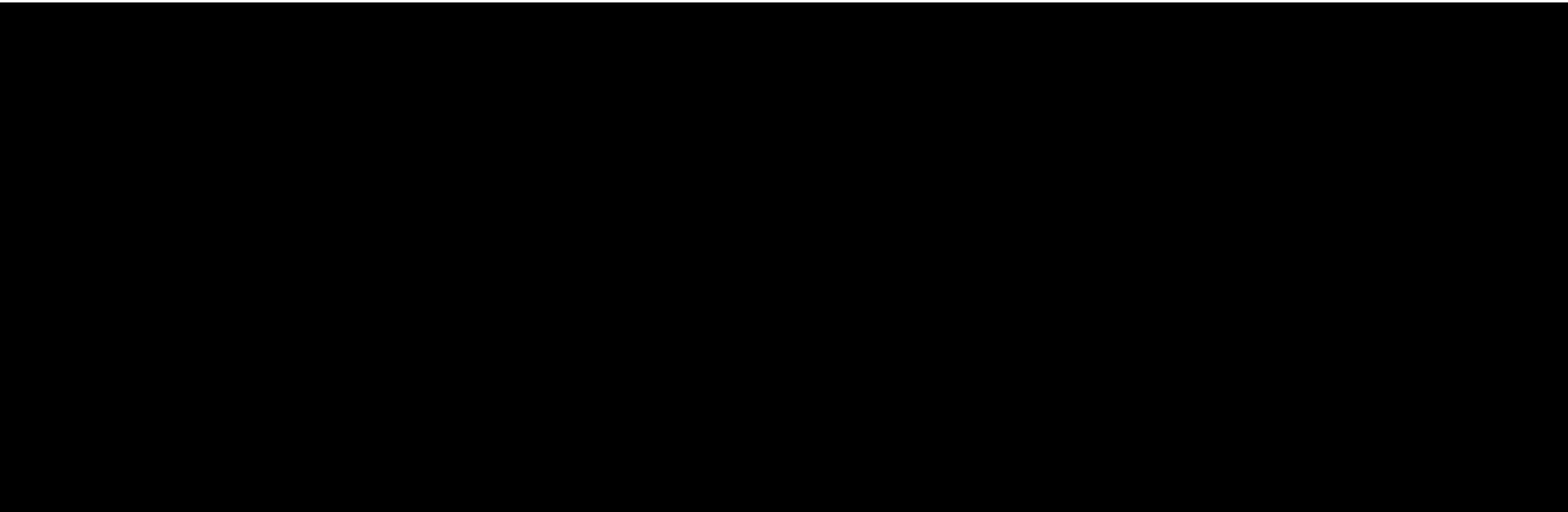
NOTE: The above Milestone dates have been updated to reflect the Contract Commencement date change (from 22nd Nov to 22nd Dec).

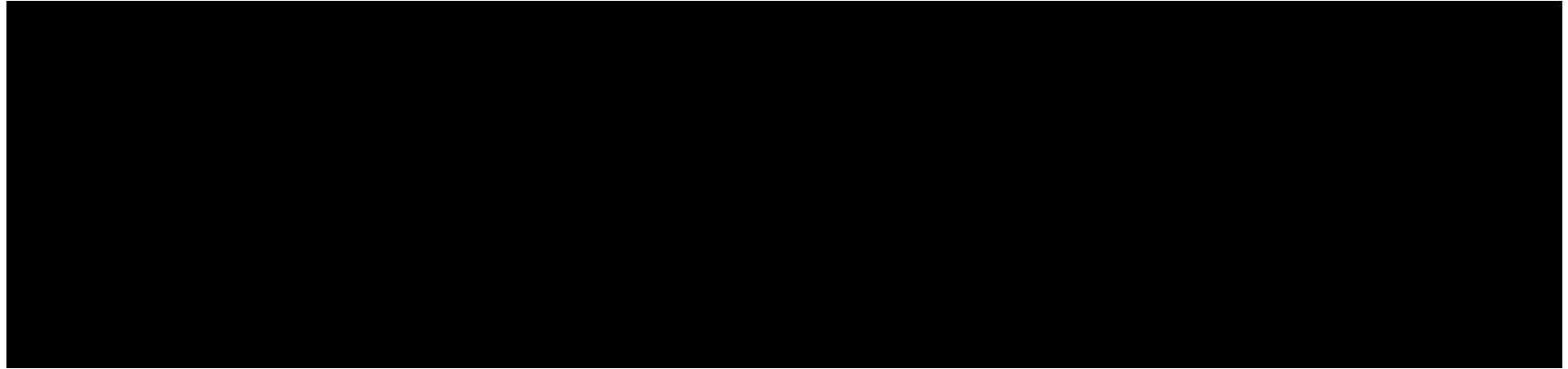
Part C – Supplier Personnel Rate Card for Calculation of Time and Materials Charges

N/A

Part D – Risk Register

Subject to the Call Off Terms, the Buyer shall not be liable for any charges or costs outside the proposed pricing within the Pricing Model. Such charges or costs include any references within the Tender Questionnaire response to any prices, costs or charges (including any potential additional prices, costs or charges; and any potential increases in prices, costs or charges relating to any risks, dependencies and assumptions) which are not included in the Pricing Model.





Part E – Early Termination Fee(s)

Any early termination fee(s) payable in accordance with the provisions of Clause 36.2 (Consequences of termination under Clauses 35.1.9 (Termination without Cause)) shall be calculated in accordance with any reasonable and proven Losses which would otherwise represent an unavoidable loss by the Supplier by reason of the termination of the Contract, provided that the Supplier takes all reasonable steps to mitigate such Losses. The Supplier shall submit a fully itemised and costed list of such Losses, with supporting evidence including such further evidence as the Buyer may require, reasonably and actually incurred by the Supplier as a result of termination under Clause 35.1.9 (Termination without Cause).

Attachment 3 – Outline Implementation Plan

The Outline Implementation Plan requirements are as set out at Appendix B - Specification and Requirements.

Attachment 4 – Service Levels and Service Credits

Service Levels and Service Credits

Service Levels and Service Credits are as set out at Annex 1 to Appendix B - Specification and Requirements.

The Service Credits shall be calculated on the basis of the formula set out at Annex 1 to Appendix B - Specification and Requirements.

Service Credit Cap

For the period of the first 12 Service Periods (inclusive), 15% of the Contract Charges payable to the Supplier for the first 12 Service Periods (inclusive); and during the remainder of the Contract Period, 20% of the Contract Charges payable to the Supplier in the period of twelve (12) months immediately preceding the month in respect of which Service Credits are accrued.

Critical Service Level Failure

A Critical Service Level Failure means a Service Level Failure for any of the following:

- a) Availability Service Level: where the Service is not Available for a consecutive period of one hour or greater in any rolling 12 consecutive Service Periods, or
- b) Availability Service Level: where the Service is not Available for less than one consecutive hour, more than once in any one Service Period, or
- c) Any three Service Levels from Service Levels SL4 to SL9 (inclusive) in any given Service Period, or
- d) Time to Fix Service Level: where the level of performance of the Supplier is less than 85% against the Measure of Service for any Priority level in any one Service Period, or
- e) Time to Fix Service Level: where the level of performance of the Supplier is less than an average of 90% against the Measure of Service for any Priority level in any rolling 12-month period.

Attachment 5 – Key Supplier Personnel and Key Sub-Contractors

- .1.1 The Parties agree that they will update this Attachment 5 periodically to record any changes to Key Supplier Personnel and/or any Key Sub-Contractors appointed by the Supplier after the Commencement Date for the purposes of the delivery of the Services.

Part A – Key Supplier Personnel

Key Supplier Personnel	Key Role(s)	Duration
		Contract Period
		Contract Period
		Contract Period
		Contract Period

Part B – Key Sub-Contractors

Attachment 6 – Software

- .1.1 The Software below is licensed to the Buyer in accordance with Clauses 20 (*Intellectual Property Rights*) and 21 (*Licences Granted by the Supplier*).
- .1.2 The Parties agree that they will update this Attachment 6 periodically to record any Supplier Software or Third Party Software subsequently licensed by the Supplier or third parties for the purposes of the delivery of the Services.

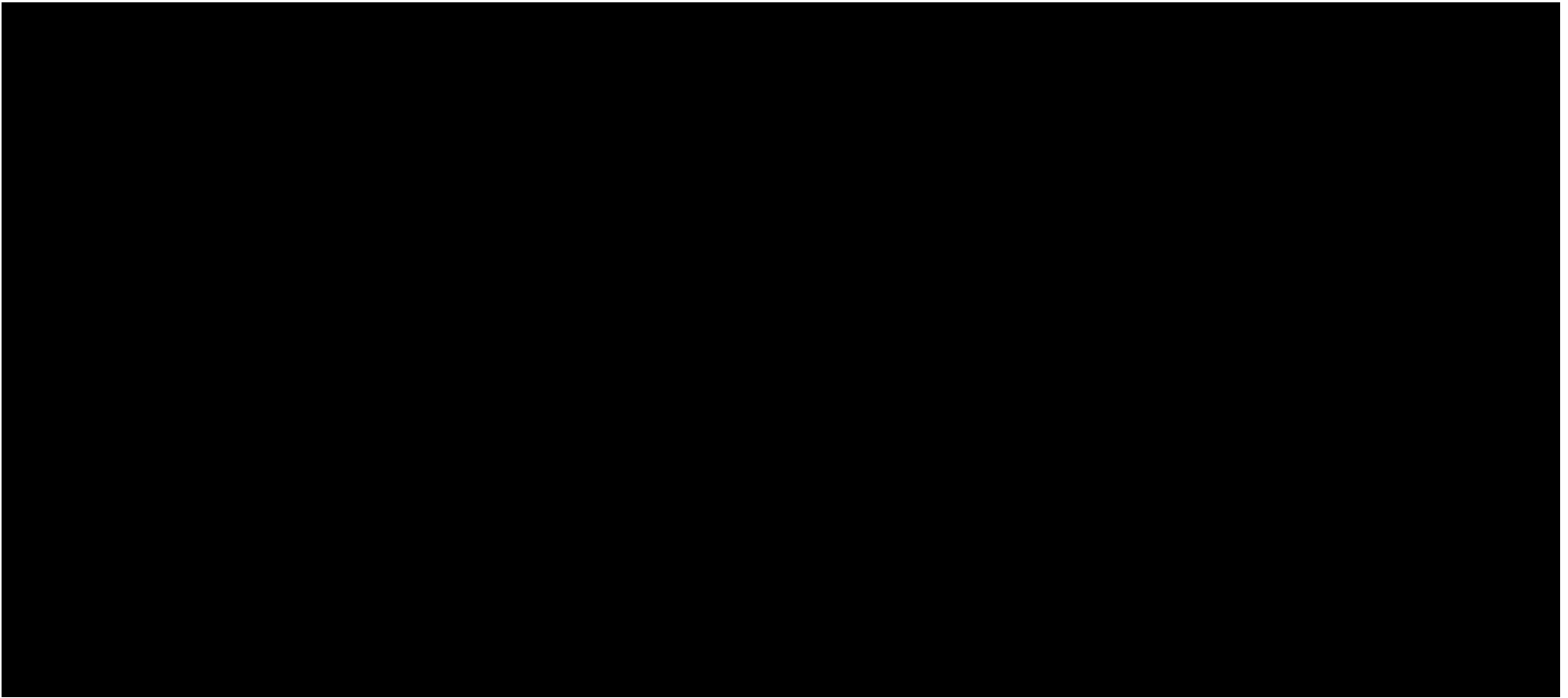
Part A – Supplier Software

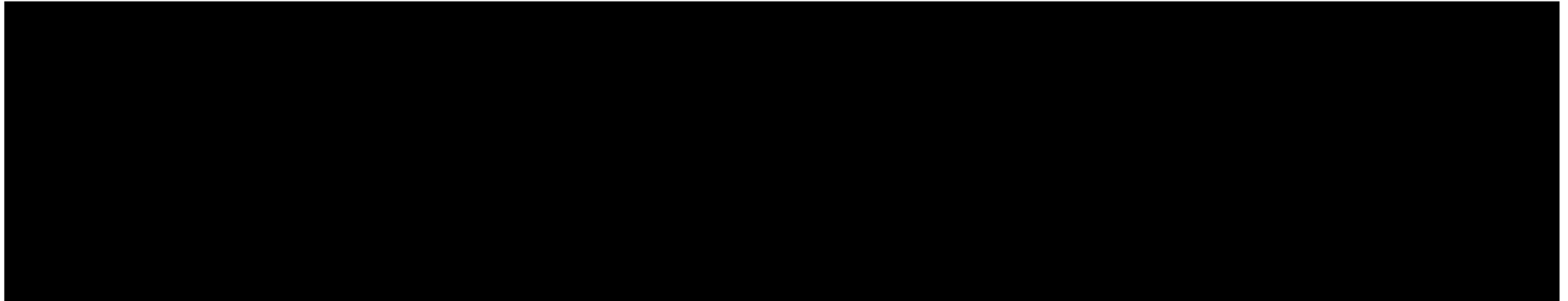
The Supplier Software includes the following items:

Software	Supplier (if an Affiliate of the Supplier)	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/ Expiry
None							

Part B – Third Party Software

The Third Party Software shall include the following items:





Attachment 7 – Financial Distress

[Redacted]

[Redacted]

[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

[Redacted]

[Redacted]

[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]

[Redacted]

[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]

PART A – SHORT FORM GOVERNANCE

For the purpose of Part A of Schedule 7 (Short Form Governance) of the Call-Off Terms, the following board shall apply:

Operational Board	
Buyer Members for the Operational Board	<div>[REDACTED]</div> <div>[REDACTED]</div> <div>[REDACTED]</div> <div>[REDACTED]</div>
Supplier Members for the Operational Board	<div>[REDACTED]</div> <div>[REDACTED]</div> <div>[REDACTED]</div> <div>[REDACTED]</div> <div>[REDACTED]</div>
Frequency of the Operational Board	Monthly, or as otherwise agreed between the Parties.
Location of the Operational Board	<div>[REDACTED]</div>

PART B – LONG FORM GOVERNANCE

For the purpose of Part B of Schedule 7 (Long Form Governance) of the Call-Off Terms, the following boards shall apply:

Service Management Board	
Buyer Members of Service Management Board (include details of chairperson)	Not Applicable
Supplier Members of Service Management Board	Not Applicable
Start Date for Service Management Board meetings	Not Applicable
Frequency of Service Management Board meetings	Not Applicable
Location of Service Management Board meetings	Not Applicable

Programme Board	
Buyer members of Programme Board (include details of chairperson)	Not Applicable
Supplier members of Programme Board	Not Applicable
Start date for Programme Board meetings	Not Applicable
Frequency of Programme Board meetings	Not Applicable
Location of Programme Board meetings	Not Applicable

Change Management Board	
Buyer Members of Change Management Board (include details of chairperson)	Not Applicable
Supplier Members of Change Management Board	Not Applicable
Start Date for Change Management Board meetings	Not Applicable
Frequency of Change Management Board meetings	Not Applicable

Location of Change Management Board meetings	Not Applicable
--	----------------

Technical Board	
Buyer Members of Technical Board (include details of chairperson)	Not Applicable
Supplier Members of Technical Board	Not Applicable
Start Date for Technical Board meetings	Not Applicable
Frequency of Technical Board meetings	Not Applicable
Location of Technical Board meetings	Not Applicable

Risk Management Board	
Buyer Members for Risk Management Board (include details of chairperson)	Not Applicable
Supplier Members for Risk Management Board	Not Applicable
Start Date for Risk Management Board meetings	Not Applicable
Frequency of Risk Management Board meetings	Not Applicable
Location of Risk Management Board meetings	Not Applicable

Attachment 9 – Schedule of Processing, Personal Data and Data Subjects

This Attachment 9 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 Schedule shall be with the Buyer at its absolute discretion.

1.1.1.1 The contact details of the Buyer's Data Protection Officer are: [REDACTED]

1.1.1.2 The contact details of the Supplier's Data Protection Officer are: [REDACTED]

1.1.1.3 The Processor shall comply with any further written instructions with respect to processing by the Controller.

1.1.1.4 Any such further instructions shall be incorporated into this Attachment 9.

Description	Details
Identity of Controller for each Category of Personal Data	<p>The Buyer is the Controller and the Supplier is the Processor.</p> <p>The Parties acknowledge that in accordance with Clause 34.2 to 34.15 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:</p> <p>The Supplier shall return and delete or securely destroy all such Personal Data and information accessed and Processed by the expiration of the Contract.</p>
Duration of the processing	For the full term of the Contract Period.
Nature and purposes of the processing	<p>The nature of the processing includes any operation such as collection, recording, organisation, structuring, compute, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) and such other processing as undertaken pursuant to the Services described in the Contract.</p> <p>The purpose of the Processing includes the specified Services as stated in the Contract including the main outcomes, responsibilities and key deliverables of the applications remediation supplier services, employment processing, statutory obligation, recruitment assessment etc.</p>
Type of Personal Data	[REDACTED]

Categories of Data Subject	
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	The Supplier shall return and delete or securely destroy all such Personal Data and information accessed and Processed by the expiration of the Contract.

Attachment 10 – Transparency Reports

Title	Content	Format	Frequency
Performance	Performance against KPIs and SLAs	Word document	Monthly
Charges	Cost and Invoicing status	Word document	Monthly
Key Sub-Contractors	Conformance against the provisions of Clause 38	Word document	Monthly
Technical	Technical monitoring statistics of the platform and infrastructure including utilisation and response times	Word document	Monthly
Performance management	Conformance against the performance requirements	Word document	Monthly

Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses

The Call Off Terms, referred to throughout this document, are substantially the terms as set out and as available from the Crown Commercial Service website:

<https://www.crowncommercial.gov.uk/agreements/rm6100>

The Additional/Alternative Schedules and Clauses, are substantially the terms as set out and as available from the Crown Commercial Service website:

<https://www.crowncommercial.gov.uk/agreements/rm6100>

Amendments to the Call Off Terms

The following amendments to the Call Off Terms are incorporated into this Contract:

Existing Clause 2.2 of the Call Off Terms is amended to read as follows:

2.2 Subject to Clauses 2.3 and 2.4 (Definitions and Interpretation), in the event and to the extent only of a conflict between the Order Form, these Call Off Terms and the provisions of the Framework, the conflict shall be resolved in accordance with the following descending order of precedence:

- 2.2.1 the Framework, except Framework Schedule 18 (Tender);
- 2.2.2 the Order Form, except Section D (Supplier Response to the Further Competition Procedure);
- 2.2.3 the amendments to the Call Off Terms as set out in the Order Form;
- 2.2.4 these Call Off Terms;
- 2.2.4 any other document referred to in the Call Off Terms;
- 2.2.5 Framework Schedule 18 (Tender);
- 2.2.6 the Collaboration Agreement (C3: Collaboration Agreement), where used; and
- 2.2.7 Section D (Supplier Response to the Further Competition Procedure) to the Order Form.

New Clause 2.4 of the Call Off Terms reads as follows:

2.4 In the event of any conflict between a Clarification and the section(s) of the Contract to which the Clarification relates, the Clarification shall take precedence.

Existing Clause 8.1 of the Call Off Terms is amended to read as follows:

- 8.1 The Supplier shall ensure that the Services:
- 8.1.1 comply in all respects with Services Specification set out or referred to in Attachment 1 (Services Specification) of the Order Form; and
 - 8.1.2 are supplied in accordance with the provisions of this Contract and, subject to Clause 2.2, are supplied in accordance with Section D (Supplier's Response to the Further Competition Procedure) to the Order Form.

Clause 15 (Charges and Invoicing) is amended as follows:

New Clauses 15.1.1 and 15.1.2 read as follows:

- 15.1.1 The Charges as described in Schedule 2 (Charges and Invoicing) and as set out in the Order Form shall include and represent the entire scope of the Services.
- 15.1.2 The Buyer shall not be responsible for any charges, costs and fees not identified in Schedule 2 (Charges and Invoicing) or the Order Form.

New Clause 36.4 (Consequences of Termination under Clause 35.1) reads as follows:

- 36.4.1 Where the Buyer terminates this Contract (or terminates any Volume Term Commitment) under Clause 35.1, the Supplier shall refund Charges related to any unused portion of any Volume Term

Commitment (less the volume discount applied to the relevant Charges in the event of termination under Clause 35.1.9 (Termination without Cause)) to the Buyer.

Schedule 1 (Definitions) is amended by the addition of the following expressions and meanings:

“Clarification”	means a point of clarification made during the Further Competition Procedure as set out at Appendix 1 (Clarifications to Supplier’s Tender) to Section D (Supplier Response to the Further Competition Procedure) and Appendix 1 (Clarifications to the Contract) to Attachment 1 (Services Specification) of the Order Form;
“SME”	means an enterprise falling within the category of micro, small and medium-sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises;
“VCSE”	means a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives.

Part A (Pricing) to Schedule 2 (Charges and Invoicing) is amended as follows:

Existing Paragraph 2.2 is deleted and shall not apply.

Part B (Charging Mechanisms) to Schedule 2 (Charges and Invoicing) is amended as follows:

Existing Paragraph 1.1 is amended to read as follows:

- 1.1 Subject to the provisions of Paragraph 1.2 of Part C of this Schedule 2 (Charges and Invoicing) in relation to the deduction of Delay Payments, on the Achievement of a Milestone, the Supplier shall be entitled to invoice the Buyer for the Milestone Payment associated with that Milestone, and where indicated in the Order Form, less an amount equal to 10% of the applicable Milestone Payment (“Retention Amount”) which may be adjusted in line with the Milestone’s Incurred Costs.

New Paragraph 1.3 reads as follows:

- 1.3 The Supplier shall be entitled to invoice the Buyer for Retention Amounts in accordance with Attachment 2 (Charges and Invoicing) of the Order Form.

New Paragraph 2.3 reads as follows:

- 2.3 The Supplier shall be entitled to submit an invoice to the Buyer for any Upfront Volume Term Commitment no earlier than thirty (30) days prior to the commencement of the Volume Term Commitment.

Part C to Schedule 2 (Charges and Invoicing) is amended as follows:

Existing Paragraph 1.1.2 is amended as follows:

"the later of" is replaced with "the earlier of". The remainder of paragraph 1.1.2 remains unchanged

Part B (Long Form Change Control Procedure) to Schedule 5 (Change Control Procedure) is amended as follows:

Existing Paragraph 2.6 is amended to read as follows:

- 2.6 At the Buyer’s request, the Supplier shall:
- [2.6.1 and 2.6.2 remain unchanged]
- 2.6.1 within 10 Working Days of the Buyer’s signature and issue of a Change Authorisation Note, deliver to the Buyer a copy of this Contract updated to reflect all Contract Changes agreed

- in the relevant Change Authorisation Note and annotated with a reference to the Change Authorisation Note pursuant to which the relevant Contract Changes were agreed; and
- 2.6.2 thereafter provide to the Buyer such further copies of the updated Contract as the Buyer may from time to time request.

Existing Variation Form is deleted and replaced with the following:

ANNEX 1 (Change Request Form) and ANNEX 2 (Change Authorisation Note) are deleted and replaced with the following:

CHANGE REQUEST FORM (ANNEX 1)	
For completion by the Party requesting the Change.	
In the event the Parties agree the Change, the Change Authorisation Note (Annex 1) only shall form the basis of the Change.	
Contract Title:	HODC Private IaaS
Contract Reference Number:	C21669
Change Request Number:	CR-[number]
Change Request Title:	
Impact Assessment required by date (where Change Request issued by the Buyer):	
Description of requested Contract Change:	
Areas of Contract impacted:	
Details of Contract Change requested (with specific reference to changes to existing Contract provisions):	
Details of any proposed alternative scenarios:	
Change required by date:	
Reasons for and benefits and disadvantages of requested Contract Change:	

Signature of requesting Change owner:	
Date of Change Request:	
IMPACT ASSESSMENT FORM	
For completion by the Supplier.	
In the event the Parties agree the Change, the Change Authorisation Note (Annex 1) only shall form the basis of the Change.	
Contract Title:	HODC Private IaaS
Contract Reference Number:	C21669
Related Change Request Number, Title and Date:	
Date of Impact assessment:	
Details of the impact of the proposed Change on the Services and the Supplier's ability to meet its other obligations under the Contract (including any impact on Service Levels, Milestones, operational service and interfaces):	
Any variation to the terms of this Contract that will be required as a result of that impact, including changes to:	
<ul style="list-style-type: none"> (a) the Services Specification and/or the Service Levels; (b) the Milestones, Implementation Plan and any other timetable previously agreed by the Parties; (c) other services provided by third party contractors to the Buyer, including any changes required by the proposed Contract Change to the Buyer's IT infrastructure; 	
Details of any relevant Specially Written Software, Supplier Software and Third Party Software to be used (including details of Software name, edition and version; purpose; number of licences; and any restrictions):	
Details any alteration in the resources, Sub-Contractors and/or to the working practices:	
A timetable for the implementation, together with any proposals for the testing of the Contract Change:	

Any proposed adjustment to the Contract Charges, including a full breakdown of costs, and any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party:

Risk assessment of the proposed Change:

Details of any underlying assumptions:

Recommendations:

Details of how the proposed Contract Change will ensure compliance with any applicable Change in Law:

Such other information as the Buyer may have reasonably requested in (or in response to) the Change request:

CHANGE AUTHORISATION NOTE (ANNEX 2)

Guidance: Change Authorisation Note **for completion by the Buyer** and signed by the Parties, in the event the Parties wish to proceed with the proposed Change.

The Contract is varied as provided within this Change Authorisation Note and shall take effect on the date signed by both Parties.

The words and expressions in this Change Authorisation Note shall have the meanings given to them in the Contract.

The Contract, including any previous Change Authorisation Note, shall remain effective and unaltered except as amended by this Change Authorisation Note.

Contract Title:	HODC Private IaaS
-----------------	-------------------

Contract Reference Number:	C21669
----------------------------	--------

Between:

The Secretary of State for the Home Department ("the Buyer")

and

[insert name of Supplier] ("the Supplier")

Change Authorisation Note Number:	CAN-[number]
-----------------------------------	--------------

Change Authorisation Note Title:	
----------------------------------	--

Date Change Authorisation Note Raised:	
Details of the Change:	
Signed by an authorised signatory to sign for and on behalf of the Buyer:	Signed by an authorised signatory to sign for and on behalf of the Supplier:
Signature:	Signature:
Name:	Name:
Position:	Position:
Date:	Date:

Part B (Long Form Security Requirements) to Schedule S3 (Security Requirements) is amended as follows:

Existing Paragraph 3.4.2 is amended to read:

3.4.2 [The ISMS shall] meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;

Existing Paragraph 3.5 is renumbered as 3.4.3.

Existing Paragraphs 3.5.1 to 3.5.10 (inclusive) are renumbered as 3.4.3.1 to 3.4.3.10, respectively.

Existing Paragraphs 3.5.11 to 3.5.13 (inclusive) are renumbered as 3.4.4 to 3.4.6, respectively.

Existing Paragraph 3.8 is amended to read:

3.8 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph **Error! Reference source not found.**2 is approved by the Buyer, [remainder of Paragraph remains unchanged.]

Existing Paragraph 3.4.2 is amended to read:

3.4.2 [The ISMS shall] meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;

Existing Paragraph 3.5.10 (renumbered as 3.4.3.10) is amended to read:

3.4.3.10 [The ISMS shall at all times provide a level of security which] complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;

Existing Paragraph 3.9 is amended to read:

3.9 Approval by the Buyer of the ISMS pursuant to Paragraph 3.3.2 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Part B Schedule S3 (Security Requirements).

Existing Paragraph 4.2.2 is amended to read:

4.2.2 [The Security Management Plan shall] comply with the Baseline Security Requirements and the Security Policy;

Existing Paragraph 5.1.4 is amended to read:

- 5.1.4 [The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect] any changes to the Security Policy;

Existing Paragraph 7.1 is amended to read:

- 7.1 The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and the Security Policy.

Existing Paragraph 9.5.4 is amended to read:

- 9.5.4 [The Supplier shall] pro-actively scan the IT Environment (to the extent that the IT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.4.5;

Schedule 6 (Transparency Reports) is amended as follows:

New Paragraphs 6 and 7 read as follows:

6. In addition to any other management information requirements set out in this Contract, the Supplier agrees and acknowledges that it shall, at no charge, provide timely, full, accurate and complete SME Transparency Reports to the Buyer which incorporate the following data:
- 6.1 the total contract revenue received directly from this contract;
 - 6.2 the total value of sub-contracted revenues under the contract (including revenues for non-SMEs/non-VCSEs); and
 - 6.3 the total value of sub-contracted revenues to SMEs and VCSEs.
- 7 The SME Transparency Reports shall be provided in the correct format as specified in Attachment 10 of the Order Form, which may be changed from time to time (including the data required) by the Buyer. The Buyer shall give at least thirty (30) days' notice in writing of any such change and shall specify the date from which it must be used.

2. Acceptance Criteria

- 2.1 Notwithstanding the provisions of the Call Off Terms, unless otherwise defined for specific Deliverables, the acceptance criteria for the Deliverables shall be error free, conform to the required specifications, standards and documentation, and conform to the Buyer's requirements as set out in the Contract.

3. Social Value

- 3.1 The Supplier shall ensure that it has an energy reduction strategy to reduce energy consumption year-on-year over the Contract Period and reduce the environmental impact of the Services through compliance with:
- 3.1.1 [Greening Government: ICT and Digital Services Strategy 2020 to 2025](#); and
 - 3.1.2 [25 Year Environment Plan \(GOV.UK\)](#).
- 3.2 The Supplier shall ensure that it has destruction and disposal policies for waste relating to the ethical and secure disposal of waste.
- 3.3 The Supplier shall comply with the provisions of ISO 14001 Environmental Management System standard or equivalent.
- 3.4 The Supplier shall consider the relevance of sustainability at all stages of the lifecycle in the provision of Services, including the consideration of commercial needs, the minimisation of negative impacts, and the maximisation of positive impacts on society and the environment.

- 3.5 The Supplier shall seek to mitigate sustainability impacts on the Services, such as the reduction of waste (paper and equipment).
- 3.6 The Supplier shall work with the Buyer to identify opportunities to introduce innovation, reduce cost and waste and ensure sustainable development is at the heart of their operation in delivering the Services.
- 3.7 The Supplier shall comply with the provisions of the Social Value Legislation in providing the Services, including social and wider economic impacts.
- 3.8 The Supplier shall develop and invest in skills development and apprenticeships to build a more skilled and productive workforce and reduce the risks of supply constraints and increased labour cost inflations.
- 3.9 The Supplier shall develop a supply chain management tracking system to ensure performance of the Contract, including prompt payment or membership of the UK Prompt Payment Code (or equivalent schemes in other countries).
- 3.14 The Supplier shall develop and implement initiatives to support staff wellbeing, including physical and mental health.
- 4. Software**
- 4.1 Where the Supplier has the responsibility to deploy or make available Software for use by the Buyer, the Supplier shall manage the deployment of Software licences for the Buyer by:
- (a) providing clear definition of the deployment method (if appropriate) and the controls in place to manage access/use the Software;
 - (b) recording Software licensing agreements, and the instances of installed Software and reporting any non-conformance to the Software licence agreements to the Buyer on a monthly basis;
 - (c) ensuring that all the necessary Software licences required for the performance of the Services are in place; and
 - (d) using appropriate discovery tools to enable the accurate and regular reporting of hardware and Software deployment and utilisation.
- 4.2 The Supplier shall be held fully liable for any non-compliance of its obligations pursuant to paragraph 4.
- 5. Definitive Media Library**
- 5.1 The Supplier shall ensure that all Software is fully and appropriately licensed in accordance with this Contract.
- 5.2 The Supplier will maintain and keep up-to-date a definitive media library ("DML") of all Software to include, but not be limited to, the following:
- (b) Software product;
 - (c) Software product version;
 - (d) Software product edition;
 - (e) Description of software product;
 - (f) Licensee;
 - (g) Licence details;
 - (h) Licence metric;
 - (i) Licence restrictions;
 - (j) Licences held;
 - (k) Date of purchase;
 - (l) Purchase agreement;
 - (m) Licence and support costs;
 - (n) Certificate of Entitlement;

- (o) Licence agreement and EULA;
- (p) Software vendor;
- (q) Supporting vendor;
- (r) Support quantity;
- (s) Support and maintenance expiry date;
- (t) Cancellation notice period;
- (u) Support agreement terms;
- (v) Owner;
- (w) Current state of licence;
- (x) aUser, administrator, and system documentation;
- (y) Details of escrow arrangements; and
- (z) Licence transfer details.

- 5.3 On a six-monthly basis, the Supplier shall audit the details in the DML to ensure its accuracy.
- 5.4 The Supplier shall provide a forward schedule of renewals highlighting their cancellation periods and ensuring the Buyer is provided at least one month's notice prior to a licence agreement's cancellation period.
- 5.5 The DML register will specifically include details about business applications provided by the Supplier. The level of information maintained about applications must be at a level that would enable a suitably qualified third party provider to locate the appropriate information to readily take on the support of the application without major impact on the Buyer business areas.
- 5.6 The Supplier shall keep a record within the DML of all completed changes to Software. This includes changes in location, configuration, usage and where the Software has been subject to a problem or Incident.
- 5.7 The Supplier shall put in place processes for the effective publishing of DML information. This publishing should be done in such a manner as to ensure that the Buyer has easy and effective access as and when it requires. A limited number of authorised Buyer users will have full read-only access to the DML.
- 5.8 The Supplier will ensure that all additions, amendments and deletions to the DML will be effectively managed.
- 5.9 The Supplier shall be held fully liable for any non-compliance of its obligations pursuant to paragraph 5.

Schedule 8 (Financial Distress) is amended as follows:

Schedule 8 now reads as follows:

1 DEFINITIONS

In this Schedule, the following definitions shall apply:

“Accounting Reference Date”	means in each year, the date to which each entity in the FDE Group prepares its annual audited financial statements;
“Applicable Financial Indicators”	means the financial indicators from Paragraph 5.1 of this Schedule which are to apply to the Monitored Suppliers as set out in Paragraph 6 of this Schedule;
“Appropriate Accepted Mitigation”	means a mitigation to a Financial Distress Event as agreed between the Parties, as follows:

- (a) as at the Effective Date, as set out in Annex 2 of this Schedule; and
- (b) during the term of the Contract, as set out in Paragraph 3.4 of this Schedule.

All Appropriate Accepted Mitigations, including any new or amended Appropriate Accepted Mitigations must be documented and recorded in a format and location agreed between the Parties, (for example, in a dedicated and access-controlled area of the Virtual Library);

“Board”

means the Supplier’s board of directors;

“Board

means written confirmation from the Board in accordance with Paragraph 8 of this Schedule;

Confirmation”

“Credit Rating Level”

means a credit rating level as specified in Annex 1 of this Schedule;

“Credit Rating Threshold”

means the minimum Credit Rating Level for each entity in the FDE Group as set out in Annex 3 of this Schedule;

“Financial Distress Event” or “FDE”

means the occurrence of one or more events as listed in Paragraph 3.1 of this Schedule;

“Financial Distress Event Group” or “FDE Group”

means the Supplier, Key Sub-contractors, the Guarantor, the Supplier’s ultimate parent undertaking, Key Sub-contractors’ ultimate parent undertakings, and the Monitored Suppliers;

“Financial Indicators”

in respect of the Supplier, Key Sub-contractors, the Guarantor, the Supplier’s ultimate parent undertaking, the Key Sub-contractors’ ultimate parent undertakings, means each of the financial indicators set out at Paragraph 5.1 of this Schedule; and in respect of each Monitored Supplier, means those Applicable Financial Indicators;

“Financial Target Thresholds”

means the target thresholds for each of the Financial Indicators set out at Paragraph 5.1 of this Schedule;

“Monitored Suppliers”

means those entities specified at Paragraph 6 of this Schedule;

“Primary Credit Ratings”

means Dun & Bradstreet credit ratings;

“Primary Credit Ratings Agency”

means Dun & Bradstreet;

“Rating Agencies”

means the rating agencies listed in Annex 1 of this Schedule or such other rating agencies as the Buyer may decide to use;

2 WARRANTIES AND DUTY TO NOTIFY

- 2.1 The Supplier warrants and represents to the Buyer for the benefit of the Buyer that as at the Effective Date:

- (a) the long-term Primary Credit Ratings issued for each entity in the FDE Group by each of the Rating Agencies are as set out in Annex 3 of this Schedule; and
- (b) either:
 - (i) the financial position or, as appropriate, the financial performance of each of the Supplier, Guarantor, Supplier's ultimate parent undertaking, Key Sub-contractors, and Key Subcontractors' ultimate parent undertakings satisfies the Financial Target Thresholds, or
 - (ii) the relevant Appropriate Accepted Mitigations are in place.

2.2 The Supplier shall promptly notify (or shall procure that its auditors promptly notify) the Buyer in writing if there is any downgrade in the credit rating issued by the Primary Credit Ratings Agency for any entity in the FDE Group, which results in the level of risk being assessed as high or greater than average (and in any event within 5 Working Days of the occurrence of the downgrade). The categorisation of credit ratings by risk level is defined in Annex 1.

2.3 The Supplier shall:

- (a) regularly monitor the credit ratings of each entity in the FDE Group with the Primary Credit Ratings Agency;
- (b) monitor and report on the Financial Indicators for each entity in the FDE Group against the Financial Target Thresholds at least quarterly, and update the Financial Indicators when public information becomes available, and in any event, no less than once a year within 285 days after the Accounting Reference Date;
- (c) provide regular updates to the Buyer on, as a minimum, the Primary Credit Ratings for each entity in the FDE Group;
- (d) promptly notify (or shall procure that its auditors promptly notify) the Buyer in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event (and in any event, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event).; and
- (e) ensure when complying with this Paragraph 2.3 that it complies with the law of England and Wales, including all market regulations and local law that applies to England and Wales.

2.4 For the purposes of determining whether a Financial Distress Event has occurred pursuant to the provisions of Paragraphs 3.1(a), the credit rating of an FDE Group entity shall be deemed to have dropped below the applicable Credit Rating Threshold if:

- (a) any of the Rating Agencies have given a Credit Rating Level for that entity which is below the applicable Credit Rating Threshold; or

- (b) a Rating Agency that is specified as holding a Credit Rating for an entity as set out at Annex 3 of this Schedule ceases to hold or is unable to provide a Credit Rating for that entity, and the Supplier fails to provide an acceptable explanation to the Buyer.

2.5 Each report submitted by the Supplier pursuant to Paragraph 2.3(b) shall:

- (a) be a single report with separate sections for each of the FDE Group entities;
- (b) contain a sufficient level of information to reasonably enable the Buyer to verify the calculations that have been made in respect of the Financial Indicators;
- (c) include key financial, explanatory narrative, and other supporting information (including any accounts data that has been relied on) as separate annexes;
- (d) be based on the audited accounts or any other publicised financial information for the date or period on which the Financial Indicator is based or, where the Financial Indicator is not linked to an accounting period or an accounting reference date, on unaudited management accounts prepared in accordance with their normal timetable; and
- (e) include a history of the Financial Indicators reported by the Supplier in graph form to enable the Buyer to easily analyse and assess the trends in financial performance.

3 FINANCIAL DISTRESS EVENTS AND APPROPRIATE ACCEPTED MITIGATIONS

3.1 The following shall be Financial Distress Events, unless an Appropriate Accepted Mitigation is in place:

- (a) the credit rating of an FDE Group entity dropping below the applicable Credit Rating Threshold;
- (b) an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;
- (c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity;
- (d) an FDE Group entity committing a material breach of covenant to its lenders;
- (e) a Key Sub-contractor notifying the Buyer that the Supplier has not satisfied any material sums properly due under a specified invoice and not subject to a genuine dispute;
- (f) any of the following:
 - (i) commencement of any litigation against an FDE Group entity with respect to financial indebtedness greater than £5m or obligations under a service contract with a total contract value greater than £5m;

- (ii) non-payment by an FDE Group entity of any financial indebtedness;
- (iii) any financial indebtedness of an FDE Group entity becoming due as a result of an event of default;
- (iv) the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity; or
- (v) the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity,

in each case which the Buyer reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance and delivery of the Services in accordance with this Agreement;

- (g) any one of the Financial Indicators set out at Paragraph 5 for any of the FDE Group entities failing to meet the required Financial Target Threshold; or
- (h) if a previously Appropriate Accepted Mitigation is no longer available for a particular FDE or is no longer sufficient to constitute an Appropriate Accepted Mitigation.

3.2 On the occurrence of an FDE pursuant to Paragraph 3.1(g) to (h):

(a) the Supplier shall:

- (i) notify the Buyer in accordance with Paragraph 22.3(d) above; and
- (ii) provide to the Buyer in writing within 10 Working Days or as otherwise agreed between the Parties of the date on which the Supplier first becomes aware of the FDE or of the date on which the Buyer has brought the FDE to the Supplier's attention, its proposed mitigation; and

(b) the Parties shall then discuss the proposed mitigation in good faith and the Buyer shall, as soon as practicable, either:

- (i) agree that the proposed mitigation constitutes an Appropriate Accepted Mitigation; or
- (ii) exercise its rights under Paragraph 4 of this Schedule.

3.3 Failure by the Buyer to exercise its rights under Paragraph 4 of this Schedule shall constitute acceptance of the Appropriate Accepted Mitigation, unless such failure was due to an act or omission of the Supplier.

3.4 For the purposes of this Paragraph 3 Appropriate Accepted Mitigations include:

(a) For the Supplier:

- (i) the existence of a valid Guarantee provided by [a Parent Undertaking] as Guarantor; and

- (ii) the Guarantor is not subject to an FDE for which there is no Appropriate Accepted Mitigation; and
 - (iii) the Supplier's ultimate parent undertaking is not subject to an FDE for which there is no Appropriate Accepted Mitigation.
 - (b) For Sub-contractors:
 - (i) The existence of a valid Guarantee provided by [a Parent Undertaking] as Guarantor; and
 - (ii) the Guarantor is not subject to an FDE for which there is no Appropriate Accepted Mitigation; and
 - (iii) the Sub-contractor's ultimate parent undertaking is not subject to an FDE for which there is no Appropriate Accepted Mitigation; and
 - (c) For all entities within the FDE Group:
 - (i) a mitigation that reduces the level of risk of the FDE to a level acceptable to the Buyer. This may include access to sufficient unused credit facilities or other risk mitigations, as listed in the Outsourcing Playbook 'Assessing and Monitoring the Economic and Financial Standing of Suppliers' Guidance note available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816634/20190710-Assessing_and_monitoring_the_economic_and_financial_standing_of_suppliers.pdf.
- 3.5 All Appropriate Accepted Mitigations including any new or amended Appropriate Accepted Mitigations will be documented and recorded in a format and location agreed between the Parties (for example in a dedicated and access-controlled area of the Virtual Library).

4 CONSEQUENCES OF FINANCIAL DISTRESS EVENTS

- 4.1 Immediately upon notification by the Supplier of a Financial Distress Event in accordance with Paragraph 22.3(d) (or if the Buyer becomes aware of a Financial Distress Event without notification and brings the event to the attention of the Supplier) and subject to Paragraph 3, the Supplier shall have the obligations and the Buyer shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.
- 4.2 In the event of the first instance within a rolling 3-month period, of a late or non-payment of a Key Sub-contractor pursuant to Paragraph 3.1, the Buyer shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier 10 Working Days to:
- (a) rectify such late or non-payment; or
 - (b) demonstrate to the Buyer's reasonable satisfaction that there is a valid reason for late or non-payment.
- 4.3 The Supplier shall (and shall procure that any Guarantor, Key Sub-contractor, Monitored Supplier, and any relevant Parent Undertaking (for the Supplier or a Key Sub-contractor) shall):

- (a) at the reasonable request of the Buyer, meet the Buyer as soon as reasonably practicable (and in any event within 3 Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Authority may permit and notify to the Supplier in writing) to review the effect of the Financial Distress Event on the continued performance and delivery of the Services in accordance with this Agreement; and
- (b) where the Authority reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3(a)) that the Financial Distress Event could impact on the continued performance and delivery of the Services in accordance with this Agreement:
 - (i) submit to the Authority for its approval, a draft Financial Distress Remediation Plan as soon as reasonably practicable (and in any event, within 10 Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Authority may permit and notify to the Supplier in writing). This draft should be consistent with the BCDR Plan and Business Continuity Plan required under Schedule 6 (Business Continuity and Disaster Recovery) AMEND AS NECESSARY; and
 - (ii) to the extent that it is legally permitted to do so and subject to Paragraph 4.8, provide such information relating to the Supplier, Guarantor, Key Sub-contractor, Monitored Supplier, and any relevant Parent Undertaking (for the Supplier or a Key Sub-contractor), as the Authority may reasonably require in order to understand the risk to the Services, which may include without limitation forecasts in relation to cash flow, orders and profits and details of financial measures being considered to mitigate the impact of the Financial Distress Event and other information that might be price sensitive.

4.4 The Authority shall not withhold its approval of a draft Financial Distress Remediation Plan unreasonably. If the Authority does not approve the draft Financial Distress Remediation Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Remediation Plan, which shall be resubmitted to the Authority within 5 Working Days of the rejection of the first draft. This process shall be repeated until the Financial Distress Remediation Plan is approved by the Authority or referred to the Dispute Resolution Procedure under Paragraph 4.5.

4.5 If the Authority considers that the draft Financial Distress Remediation Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not ensure the continued performance of the Supplier's obligations in accordance with the Agreement, then it may either agree a further time period for the development and agreement of the Financial Distress Remediation Plan or escalate any issues with the draft Financial Distress Remediation Plan using the Dispute Resolution Procedure.

4.6 Following approval of the Financial Distress Remediation Plan by the Authority, the Supplier shall:

- (a) on a regular basis (which shall not be less than fortnightly):

- (i) review and make any updates to the Financial Distress Remediation Plan as the Supplier may deem reasonably necessary and/or as may be reasonably requested by the Authority, so that the plan remains adequate, up to date and ensures the continued performance and delivery of the Services in accordance with this Agreement; and
 - (ii) provide a written report to the Authority setting out its progress against the Financial Distress Remediation Plan, the reasons for any changes made to the Financial Distress Remediation Plan by the Supplier and/or the reasons why the Supplier may have decided not to make any changes;
 - (b) where updates are made to the Financial Distress Remediation Plan in accordance with Paragraph 4.6(a), submit an updated Financial Distress Remediation Plan to the Authority for its approval, and the provisions of Paragraphs 4.4 and 4.5 shall apply to the review and approval process for the updated Financial Distress Remediation Plan; and
 - (c) comply with the Financial Distress Remediation Plan (including any updated Financial Distress Remediation Plan).
- 4.7 Where the Supplier reasonably believes that the relevant Financial Distress Event under Paragraph 4.1 (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify the Authority and the Parties may agree that the Supplier shall be relieved of its obligations under Paragraph 4.6.
- 4.8 The Supplier shall use reasonable endeavours to put in place the necessary measures to ensure that the information specified at Paragraph 4.3(b)(ii) is available when required and on request from the Authority and within reasonable timescales. Such measures may include:
- (a) obtaining in advance written authority from Key Sub-contractors, the Guarantor, Monitored Suppliers, and any relevant Parent Undertaking (for the Supplier or a Key Sub-contractor) authorising the disclosure of the information to the Authority and/or entering into confidentiality agreements which permit disclosure;
 - (b) agreeing in advance with the Authority, Key Sub-contractors, the Guarantor Monitored Suppliers, and any relevant Parent Undertaking (for the Supplier or a Key Sub-contractor) a form of confidentiality agreement to be entered by the relevant parties to enable the disclosure of the information to the Authority;
 - (c) putting in place any other reasonable arrangements to enable the information to be lawfully disclosed to the Authority (which may include (without limitation) making information available to nominated Authority personnel through confidential arrangements, subject to their consent); and
 - (d) disclosing the information to the fullest extent that it is lawfully entitled to do so, including through the use of redaction, anonymization and any other techniques to permit disclosure of the information without breaching a duty of confidentiality.

5 FINANCIAL INDICATORS

5.1 Subject to the calculation methodology set out at Annex 4 of this Schedule, the Financial Indicators and the corresponding calculations and thresholds used to determine whether a Financial Distress Event has occurred in respect of those Financial Indicators, shall be as follows:

Financial Indicator	Calculation ¹	Financial Target Threshold:	2.4 Monitoring and Reporting Frequency (if different from the default position set out in Paragraph 2.3(b))
1 The higher of (a) the Operating Margin for the most recent 12-month period and (b) the average Operating Margin for the last two 12-month periods	<i>Operating Margin = Operating Profit / Revenue</i>	> 5%	Tested and reported at least quarterly in arrears based on the latest publicly available information. Calculation as a minimum should be updated within 285 days of each Accounting Reference Date based upon figures for the 12 months ending on the relevant accounting reference date.
2 Net Debt to EBITDA Ratio	<i>Net Debt to EBITDA ratio = Net Debt / EBITDA</i>	< 3.5 times	Tested and reported at least quarterly in arrears based on latest publicly available information. Calculation as a minimum should be updated within 285 days of each accounting reference date based upon EBITDA for the 12 months ending on, and Net Debt at, the relevant accounting reference date
3 Net Debt + Net Pension Deficit to EBITDA ratio	<i>Net Debt + Net Pension Deficit to EBITDA Ratio = (Net Debt + Net Pension Deficit) / EBITDA</i>	< 5 times	Tested and reported quarterly in arrears based on latest publicly available information. Calculation as a minimum should be updated within 285 days of each accounting reference date based upon EBITDA for the 12 months ending on, and the Net Debt and Net Pension Deficit at, the relevant accounting reference date.

4 Net Interest Cover	<i>Net Interest Payable Cover = Earnings Before Interest and Tax / Net Interest Payable</i>	> 3 times	Tested and reported at least quarterly in arrears based on latest publicly available information. Calculation as a minimum should be updated within 285 days of each accounting reference date based upon figures for the 12 months ending on the relevant accounting reference date.
5 Current Ratio	Current Ratio = Current Assets / Current Liabilities	> 1 times	Tested and reported quarterly in arrears based on latest publicly available information. Calculation as a minimum should be updated within 285 days of each accounting reference date based upon figures at the relevant accounting reference date.
6 Net Asset value	<i>Net Asset Value = Net Assets</i>	> £0	Tested and reported quarterly in arrears based on latest publicly available information. Calculation as a minimum should be updated within 285 days of each accounting reference date based upon figures at the relevant accounting reference date.
.2.26 7 Group Exposure Ratio	<i>Group Exposure Ratio = Current Assets – Group Assets – Current Liabilities</i>	> £0 If lower a PCG may be required	Tested and reported quarterly in arrears based on the latest publicly available information. Calculation as a minimum should be updated within 285 days of each accounting reference date based upon figures at the relevant accounting reference date.
8 Free Reserve Ratio	.2.31 Free Reserve Ratio = Free Reserves / Unrestricted Expenditure	.2.33 > 0.25	Tested and reported at least quarterly in arrears based on the latest available information. Calculation as a minimum should be updated within 285 days of each accounting reference date based upon figures at the relevant accounting reference date.

.2.37 Key: ¹ – See Annex 4 of this Schedule which sets out the calculation methodology to be used in the calculation of each Financial Indicator.

6 MONITORED SUPPLIERS

6.1 Monitored Suppliers shall be designated at contract signature.

6.2 A Monitored Supplier could include any Sub-contractor that is not a key subcontractor, which in the opinion of the Authority, performs (or would perform if appointed) a role:

- (a) in the provision of all or any part of the Services that is such that the discontinued provision of that role would be detrimental to the ability of the Supplier to deliver the Services to its established performance standards; and/or
- (b) in the provision of all or any part of the Services that is such that the discontinued provision of that role may affect the Supplier's financial stability; and/or
- (c) for which it would be difficult for the Supplier to find a replacement Sub-contractor within a reasonable time.

Monitored Supplier	Applicable Financial Indicators (these are the Financial Indicators from the table in Paragraph 5.1 which are to apply to the Monitored Suppliers)
[COMPLETE AS REQUIRED]	[COMPLETE AS REQUIRED]

.3

7 TERMINATION RIGHTS

7.1 The Authority shall be entitled to terminate this Contract under Clause 35.2 (*Termination by the Authority*) if:

- (a) the Supplier fails to notify the Authority of a Financial Distress Event in accordance with Paragraph 2.3(c);
- (b) the Parties fail to agree a Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraphs 4.3 to 4.5; and/or
- (c) the Supplier fails to comply with the terms of the Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraph 4.6(c).

8 BOARD CONFIRMATION

- 8.1 If this Contract has been specified as a Critical Service Contract then, subject to Paragraph 8.4 of this Schedule, the Supplier shall within 120 days after each Accounting Reference Date or within 15 months of the previous Board Confirmation (whichever is the earlier) provide a Board Confirmation to the Authority in the form set out at Annex 5 of this Schedule, confirming that to the best of the Board's knowledge and belief, it is not aware of and has no knowledge:
- (a) that a Financial Distress Event has occurred since the later of the Effective Date or the previous Board Confirmation or is subsisting; or
 - (b) of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event.
- 8.2 The Supplier shall ensure that in its preparation of the Board Confirmation it exercises due care and diligence and has made reasonable enquiry of all relevant Supplier Personnel and other persons as is reasonably necessary to understand and confirm the position.
- 8.3 In respect of the first Board Confirmation to be provided under this Agreement, the Supplier shall provide the Board Confirmation within 15 months of the Effective Date if earlier than the timescale for submission set out in Paragraph 8.1 of this Schedule.
- 8.4 Where the Supplier is unable to provide a Board Confirmation in accordance with Paragraphs 8.1 to 8.3 of this Schedule due to the occurrence of a Financial Distress Event or knowledge of subsisting matters which could reasonably be expected to cause a Financial Distress Event, it will be sufficient for the Supplier to submit in place of the Board Confirmation, a statement from the Board of Directors to the Authority (and where the Supplier is a Strategic Supplier, the Supplier shall send a copy of the statement to the Cabinet Office Markets and Suppliers Team) setting out full details of any Financial Distress Events that have occurred and/or the matters which could reasonably be expected to cause a Financial Distress Event.

ANNEX 1: RATING AGENCIES AND THEIR STANDAR RATING SYSYTEM

This Annex sets out the standard rating scales for each of the Rating Agencies selected. The Authority reserves the right to use other rating scales from other Rating Agencies that are not listed in this Annex.

Rating Agency	Credit Rating Level	Risk level
Standard and Poor's	Credit Rating Level 1 = [AAA] [AA+] [AA] [AA-] [A+] [A] [A-]	Low Risk
	Credit Rating Level 2 = [BBB+] [BBB] [BBB-] [BB+] [BB] [BB-] [B+] [B] [B-]	Greater Than Average Risk
	Credit Rating Level 3 = [CCC] [CC] [C] [D] [NR]	High Risk

Moody's	Credit Rating Level 1 = [Aaa] [Aa] [A]	Low Risk
	Credit Rating Level 2 = [Baa] [Ba] [B]	Greater Than Average Risk
	Credit Rating Level 3 = [Caa] [Ca] [C]	High Risk
Dun and Bradstreet	Credit Rating Level 1 = Failure Score of 51 or above	Low Risk
	Credit Rating Level 2 = Failure Score of 11 to 50	Greater Than Average Risk
	Credit Rating Level 3 = Failure Score of 10 or below	High Risk
Experian	Credit Rating Level 1 = 51 or above	Low Risk
	Credit Rating Level 2 = 26 to 50	Greater Than Average Risk
	Credit Rating Level 3 = 25 or below	High Risk
Companywatch	Credit Rating Level 1 = 36 and above	Low Risk
	Credit Rating Level 2 = 26 to 35	Greater Than Average Risk
	Credit Rating Level 3 = 25 or below	High Risk

ANNEX 2: APPROPRIATE ACCEPTED MITIGATIONS

1. As at the Effective Date, the Parties agree that the Appropriate Accepted Mitigation:

(a) For the Supplier is the continued access to unused credit facilities that are in excess of the sum of Current Liabilities less Current Assets.

ANNEX 3: Credit Ratings And Credit Rating Thresholds

Entity	Credit Rating (long term) <i>(insert the actual credit rating issued for the entity at the Effective Date)</i>	Credit Rating Threshold <i>(insert the minimum actual rating (e.g. AA-) or the minimum Credit Rating Level (e.g. Credit Rating Level 3))</i>
<div></div>		

ANNEX 4: Calculation Methodology for Financial Indicators

- .3.1 The Supplier shall ensure that it uses the following general and specific methodologies for calculating the Financial Indicators against the Financial Target Thresholds:

General methodology

1. **Terminology:** The terms referred to in this Annex are those used by UK companies in their financial statements. Where the entity is not a UK company, the corresponding items should be used even if the terminology is slightly different (for example a charity would refer to a surplus or deficit rather than a profit or loss).
2. **Groups:** Where the entity is the holding company of a group and prepares consolidated financial statements, the consolidated figures should be used.
3. **Foreign currency conversion:** Figures denominated in foreign currencies should be converted at the exchange rate in force at the relevant date for which the Financial Indicator is being calculated.
4. **Treatment of non-underlying items:** Financial Indicators should be based on the figures in the financial statements before adjusting for non-underlying items.

Specific Methodology

Financial Indicator	Specific Methodology
1 <u>Operating Margin</u>	The elements used to calculate the Operating Margin should be shown on the face of the Income Statement (or Statement of Financial

	<p>Activities) in a standard set of financial statements.</p> <p>Operating Profit is to exclude exceptional items, such as restructuring costs or impairments, and to include any share of Subsidiaries' Operating Profit.</p> <p>Where an entity has an operating loss (i.e. where the operating profit is negative), Operating Profit should be taken to be zero.</p> <p>For Charities Operating Profit would be Net Income or Expenditure after Charitable Activities / Income</p>
<p>2</p> <p><u>Net Debt to EBITDA Ratio</u></p>	<p><i>"Net Debt"</i> = Bank overdrafts + Loans and borrowings + Finance leases + Deferred consideration payable – Cash and cash equivalents</p> <p><i>"EBITDA"</i> = Operating profit + Depreciation charge + Amortisation charge. EBITDA is to exclude exceptional items, such as restructuring costs or impairments, and to include any share of Subsidiaries' EBITDA.</p> <p>The majority of the elements used to calculate the Net Debt to EBITDA Ratio should be shown on the face of the Balance sheet, Income statement (or Statement of Financial Activities) and Statement of Cash Flows in a standard set of financial statements but will otherwise be found in the notes to the financial statements.</p> <ul style="list-style-type: none"> • <i>Net Debt:</i> The elements of Net Debt may be described slightly differently and should be found either on the face of the Balance Sheet or in the relevant note to the financial statements. All interest-bearing liabilities (other than retirement benefit obligations) should be included as borrowings as should, where disclosed, any liabilities (less any assets) in respect of any hedges designated as linked to borrowings (but not non-designated hedges). Borrowings should also include balances owed to other group members. <p>Deferred consideration payable should be included in Net Debt despite typically being non-interest bearing.</p> <p>Cash and cash equivalents should include short-term financial investments shown in current assets.</p>

	<p>Where Net debt is negative (i.e. an entity has net cash), the relevant Financial Target Threshold should be treated as having been met.</p> <p><i>EBITDA</i>: Operating profit should be shown on the face of the Income Statement (or Statement of Financial Activities) and, for the purposes of calculating this Financial Indicator. <i>The depreciation and amortisation charges for the period may be found on the face of the Statement of Cash Flows or in a Note to the Accounts. Where EBITDA is negative, the relevant Financial Target Threshold should be treated as not having been met (unless Net Debt is also negative, in which case the relevant Financial Target Threshold should be treated as having been met).</i></p> <p>For Charities Operating Profit would be Net Income or Expenditure after Charitable Activities / Income</p>
<p>3</p> <p>[Net Debt + Net Pension Deficit to EBITDA ratio]</p>	<p><i>“Net Debt”</i> = Bank overdrafts + Loans and borrowings + Finance leases + Deferred consideration payable – Cash and cash equivalents</p> <p><i>“Net Pension Deficit”</i> = Retirement Benefit Obligations – Retirement Benefit Assets</p> <p><i>“EBITDA”</i> = Operating profit + Depreciation charge + Amortisation charge. <i>EBITDA is to exclude exceptional items, such as restructuring costs or impairments, and to include any share of Subsidiaries’ EBITDA.</i></p> <p>The majority of the elements used to calculate the Net Debt + Net Pension Deficit to EBITDA Ratio should be shown on the face of the Balance sheet, Income statement (or Statement of Financial Activities) and Statement of Cash Flows in a standard set of financial statements but will otherwise be found in the notes to the financial statements.</p> <ul style="list-style-type: none"> • <u>Net Debt</u>: The elements of Net Debt may be described slightly differently and should be found either on the face of the Balance Sheet or in the relevant note to the financial statements. All interest-bearing liabilities

(other than retirement benefit obligations) should be included as borrowings as should, where disclosed, any liabilities (less any assets) in respect of any hedges designated as linked to borrowings (but *not* non-designated hedges). Borrowings should also include balances owed to other group members.

Deferred consideration payable should be included in Net Debt despite typically being non-interest bearing.

Cash and cash equivalents should include short-term financial investments shown in current assets.

- Net Pension Deficit: Retirement Benefit Obligations and Retirement Benefit Assets may be shown on the face of the Balance Sheet or in the notes to the financial statements. They may also be described as pension benefits / obligations, post-employment obligations or other similar terms.

Where 'Net Debt + Net Pension Deficit' is negative, the relevant Financial Target Threshold should be treated as having been met.

- EBITDA: Operating profit should be shown on the face of the Income Statement (or Statement of Financial Activities) and, for the purposes of calculating this Financial Indicator.

The depreciation and amortisation charges for the period may be found on the face of the Statement of Cash Flows or in a Note to the Accounts.

Where EBITDA is negative, the relevant Financial Target Threshold should be treated as not having been met (unless 'Net Debt + Net Pension Deficit' is also negative, in which case the relevant Financial Target Threshold should be regarded as having been met).

For Charities Operating Profit would be Net Income or Expenditure after Charitable Activities / Income

<p>4</p> <p>Net Interest Payable Cover</p>	<p><i>“Earnings Before Interest and Tax”</i> = Operating profit</p> <p><i>“Net Interest Payable”</i> = Interest payable – Interest receivable</p> <p>Operating profit should be shown on the face of the Income Statement (or Statement of Financial Activities) in a standard set of financial statements. Operating Profit is to exclude exceptional items, such as restructuring costs or impairments, and to include any share of Subsidiaries’ Operating Profit</p> <p>Interest receivable and interest payable should be shown on the face of the Cash Flow statement.</p> <p>Where Net interest payable is negative (i.e. the entity has net interest receivable), the relevant Financial Target Threshold should be treated as having been met.</p> <p>For Charities Operating Profit would be Net Income or Expenditure after Charitable Activities / Income</p>
<p>5</p> <p>Current Ratio</p>	<p>All elements that are used to calculate the Current Ratio are available on the face of the Balance Sheet in a standard set of financial statements.</p>
<p>6</p> <p>Net Asset value</p>	<p>Net Assets are shown (but sometimes not labelled) on the face of the Balance Sheet of a standard set of financial statements. Net Assets are sometimes called net worth or ‘Shareholders’ Funds’. They represent the net assets available to the shareholders. Where an entity has a majority interest in another entity in which there are also minority or non-controlling interests (i.e. where it has a subsidiary partially owned by outside investors), Net Assets should be taken inclusive of minority or non-controlling interests (as if the entity owned 100% of such entity).</p> <p>For Charities Net Assets would be Total Charity Funds</p>
<p>7</p> <p>Group Exposure Ratio</p>	<p><i>“Group Assets”</i> = Current and Non-Current Balances owed by Group Undertakings</p> <p><u>Group Exposure</u>: Balances owed by (i.e. receivable from) Group Undertakings are shown</p>

	<p>within Non-Current assets or Current assets either on the face of the Balance Sheet or in the relevant notes to the financial statements. In many cases there may be no such balances, in particular where an entity is not a member of a group or is itself the ultimate holding company of the group.</p> <p><u>Current Assets & Current Liabilities:</u> Both Current assets and Current Liabilities are shown on the face of the Balance Sheet</p>
<p>8</p> <p>Free Reserve Ratio</p>	<p><u>“Free Reserves” = Unrestricted Reserves – Designated Reserves (Unless these are for Continuity purposes) – Non-cashable Assets (e.g. PPE, Intangible Assets etc.)</u></p> <p>Expenditure is shown on the face of the Income Statement (or Statement of Financial Activities)</p>

ANNEX 5: BOARD CONFIRMATION

Supplier Name: Exponential-e
Contract Reference Number: C21669

The Board of Directors acknowledge the requirements set out at Paragraph 8 of Schedule 8 (Financial Distress) and confirm that the Supplier has exercised due care and diligence and made reasonable enquiry of all relevant Supplier Personnel Staff and other persons as is reasonably necessary to enable the Board to prepare this statement. The Board of Directors confirms, to the best of its knowledge and belief, that as at the date of this Board Confirmation it is not aware of and has no knowledge:

1. that a Financial Distress Event has occurred since the later of the previous Board Confirmation and the Effective Date or is subsisting; or
2. of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event

On behalf of the Board of Directors:

Chair
Signed
Date 22nd December 2021

Director
Signed
Date 22nd December 2021



