



**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 01/04/2024 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 RM6100 Technology Services 3. 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. Appendix 1 - ICT Acceptable Use and Access Control Policy
13. Appendix 2 – Tender Response
14. Appendix 3 - ICT Operational Services ITT clarifications

The Order of Precedence shall be as set out in Clause 2.2 of the Call-Off Terms being:

1. the Framework, except Framework Schedule 18 (Tender);



2. the Order Form;
3. the Call Off Terms; and
4. Framework Schedule 18 (Tender).

Section A

General information

Contract Details	
Contract Reference:	Proc-732-2023
Contract Title:	ICT Operational Services
Contract Description:	The Competition Markets Authority (CMA) requires a strategic partner to help provide ICT operational support services.
Contract Anticipated Potential Value: this should set out the total potential value of the Contract	£600,000
Estimated Year 1 Charges:	£300,000
Commencement Date: this should be the date of the last signature on Section E of this Order Form	21/03/24

Buyer details

Buyer organisation name

Competition and Markets Authority

Billing address

Your organisation's billing address - please ensure you include a postcode

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

Buyer representative name

The name of your point of contact for this Order

[REDACTED]

Buyer representative contact details



Crown
Commercial
Service

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.

Proc-732-2023

Supplier details

Supplier name

The supplier organisation name, as it appears in the Framework Agreement

Methods Business and Digital Technology Limited.

Supplier address

Supplier's registered address

Supplier representative name

The name of the Supplier point of contact for this Order

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.

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.



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 | X |
| b: Operational Management | <input 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

24

Extension Period (Optional) Months

12 + 12 + 12

Minimum Notice Period for exercise of Termination Without Cause:

30 (Calendar days) (see Clause 35.1.9 of the Call-Off Terms)

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]

Buyer Assets

Per Supplier resource:

1x CMA laptop
1x CMA mobile

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.

ITIL

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.

N/A

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.

See Appendix 1 – ICT Acceptable Use and Access Control Policy (May 2023)

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 (£) – N/A

Professional Indemnity Insurance (£) – N/A

Buyer Responsibilities

Guidance Note: list any applicable Buyer Responsibilities below.

The Buyer will provide the Supplier with CMA laptops and mobile phones to provide effective support for CMA customers.



The Buyer will set up appropriate access to its premises for each of the supplier's resources.

Goods

Guidance Note: list any Goods and their prices.

N/A

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 checked="" type="checkbox"/>
Part B – Long Form Change Control Schedule	<input type="checkbox"/>

The Part selected above shall apply this Contract.



Crown
Commercial
Service

Section C

Part A - Additional and Alternative Buyer Terms

N/A



Section D Supplier Response

Please see the supplier response in Appendix 2 - Supplier Response, issued by the Supplier 05/01/2024

Commercially Sensitive information

Any confidential information that the Supplier considers sensitive for the duration of an awarded Contract should be included here. Please refer to definition of Commercially Sensitive Information in the Contract – *use specific references to sections rather than copying the relevant information here.*

- 13. Appendix 2 > Stage 2 Quality Questions (Page 59 – 74)
- 13. Appendix 2 > Stage 3 Price Information (Page 75 - 78)



Section E Contract Award

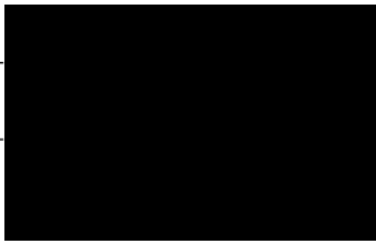
This Call Off Contract is awarded in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100.

SIGNATURES

For and on behalf of the Supplier

Name		
Job role/title		
Signature		
Date	21/03/2024	

For and on behalf of the Buyer

Name		
Job role/title		
Signature		
Date	15/03/2024	



Attachment 1 – Services Specification

1. Overview of Services:

1.1. The supplier will provide ICT operational support services as follows:

	Service Desk / AV support	EUC Rollout engineer
Core services	<ul style="list-style-type: none"> • providing onsite first/second line IT support services (including AV support) in the CMA Manchester office. • visiting other CMA locations (this will equate to 2 days per month). 	<ul style="list-style-type: none"> • providing project rollout services to the End User Computing team (such projects include upgrading and replacing staff mobile phones and laptops).
Optional services	<ul style="list-style-type: none"> • optional out of hours support. • optional consultancy services to help improve IT operational services. 	

1.2. The Supplier will be expected to:

- Support CMA staff in a hybrid environment including remote troubleshooting.
- Respond to desk walk-ups.
- Manage local joiner and leaver activities including equipment deployment / collections, user setup and IT induction training,
- Software deployment and subsequent configuration.
- Foster relationships and collaborate with other external contractors in restoring business services in an event of a major incident or outage.
- Manage IT hardware including maintain stock levels to honour any future replacement requests or joiner deployments., laptop/phone builds, deploy replacement items and manage repairs with 3rd party suppliers.
- Provide AV 1st line support.
- Produce and update knowledgebase articles/training material relevant to the site of occupancy.
- Provide comprehensive reports to cover any damaged site equipment detailing date, time stamp, nature of damage.
- Report on any damaged user equipment following the CMA ServiceDesk tool (currently TopDesk) process. This will include desk monitors, AV equipment, laptops, tablets and any other equipment of high value as such mentioned above.
- Cover in the event of any planned form of absence, illness or unforeseen circumstances.
- Seek to continuously improve service delivered itself (and to help the wider CMA IT function to improve).



- The Supplier will use CMA systems to deliver the required services.

- 1.3. The Supplier will need to align practises to existing CMAs ServiceDesk operation ways of working. It is important to note that at present CMA's ITSM tool is used to record customer satisfaction, which is consistently above 90% across all CMA offices where there is Service Desk presence. The same expectation will be applied to the Supplier.
- 1.4. In an event where the performance or experience of one or more of the Supplier's provided resource(s) is deemed as unsatisfactory by the Buyer, a meeting will be held to discuss the concerns. If the Supplier is unable to resolve the Buyer's concerns in the agreed timescales then the Buyer reserves the right to request alternative resource(s) from the Supplier. Unless agreed otherwise, when the Buyer requests an alternative resource from the Supplier the underperforming resource will no longer work with the Buyer beyond the agreed timescales

2. Requirements

2.1. Requirements - ServiceDesk / AV Support

- 2.1.1. In order to effectively deliver these operational services, the Buyer requires:

Ref	Requirement
R1.1	Experience of working in an IT support role, with familiarity of IT Service Management tools; or completed an ITIL Foundation, Level 2 or Level 3 End User Computing qualification.
R1.2	All analysts to hold a security vetting level of Security Clearance (SC)
R1.3	One (1) named <u>onsite</u> Service Desk support resources at our Manchester office to floorwalk as the building opens / staff occupy the building.
R1.4	One (1) named <u>onsite</u> Service Desk support resource at our Manchester office throughout the initial two term year.
R1.5	Up to four (4) EUC Rollout engineers to work on hardware refresh projects.
R1.6	The ServiceDesk office hours, Monday – Friday 8am-6pm (excluding English public and bank holidays). However, support will be required between the hours of 9am – 5pm
R1.7	Sickness and holiday cover must be provided for the onsite resources
R1.8	Option to deploy skilled 1 st / 2 nd line resources to other CMA offices, when required with a minimum of 1 weeks notice.



2.1.2. Below is the experience and skills required for resources to provide first and second line support for customer service for end-users in line with ITIL service management model. This includes ServiceDesk and AV support activities.

Ref	Requirement
R2.1	Experience of working in an IT support role, with familiarity of IT Service Management tools; or completed an ITIL Foundation, Level 2 or Level 3.
R2.2	Experience and/or knowledge of working with AV equipment, video conferencing configuration and setup.
R2.3	Well-developed IT skills with proven knowledge of Microsoft Office with a focus on Microsoft365
R2.4	Significant knowledge and/or experience deploying end user devices such as laptops, tablets, mobile phones, basic troubleshooting of AV equipment.
R2.5	Good communication, and excellent customer service skills, with the ability to work collaboratively with business users and staff at various levels.
R2.6	Excellent organisational skills, with the ability to prioritise key actions and ensure delivery to specification and deadlines.
R2.7	An End User Computing qualification.
R3.1	To act as the first point of contact for IT-related incidents by logging, prioritising, and taking ownership of assigned issues until closure. Ensuring timely resolution to minimise disruption to the users. All incidents must be resolved within the agreed CMA internal service level agreements (SLAs) using the CMA ITSM tool (TOPdesk)
R3.2	To honour various service requests such as software installations, access requests, hardware provisioning, password resets whilst adhering to CMA internal processes. Ensuring these requests are properly logged, prioritised, and fulfilled within agreed-upon service level agreements (SLAs) using the CMA ITSM tool (TOPdesk)
R3.3	To ensure CMA assets are documented and recorded in accordance to internal processes thereby maintaining accurate inventory whilst using the appropriate toolset. To ensure an audit trail is visible when hardware or software is updated or replaced.
R3.4	To assist in maintaining the CMA's knowledge base database by creating, documenting and updating solutions, known errors, workarounds, and frequently asked questions for end-users and other ServiceDesk analysts.



Ref	Requirement
R3.5	To provide an excellent service by improving upon service delivery and customer engagement which are essential to the CMA's service provision. To maintain positive feedback response through our customer satisfaction module which requires quality support to all CMA users.
R3.6	All levels of support will adhere to the CMA established SLAs for incident management and service request fulfilment.
R3.7	Provide on-site presence for the provision of support and/or fixing faults.
R3.8	Provide first line support for Audio visual system by ensure the availability and reliability of AV equipment and systems to facilitate seamless communication and collaboration within the organization.
R3.9	Provide timely and effective technical support for AV-related issues, including setup, configuration and troubleshooting.
R3.10	Troubleshooting and diagnosis of audio and video quality issues
R3.11	Assistance with AV setups for meetings, conferences, presentations, and events.
R3.12	Training and support for end-users on AV equipment operation and best practices
R3.13	On-site support during events to ensure smooth operation of AV equipment.
R3.14	Assistance with video conferencing and remote participation capabilities
R3.15	Provide out-of-hour support services

2.2. Requirements - Project Rollout Engineer

- 2.2.1. As part of the CMA EUC strategy, the CMA require support for large projects EUC refresh projects under this contract. End user device refresh projects allow the CMA to enhance productivity, efficiency, and compatibility with the latest technology standards.
- 2.2.2. In the FY 2023/24, the CMA's EUC team plan to undertake a laptop and mobile handset refresh of approximately 400 laptop and 400 mobile handsets. As part of this contract, The CMA require roll-out engineers to work the CMA on this project. A

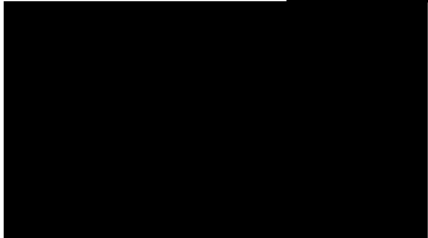


similar project may also take place in FY24/25 but the CMA gives no guarantee on levels of use.

2.2.3. Below are the skills required for resources required to provide support for large projects:

Ref	Requirement
R4.1	Experience of provisioning End user devices such as laptops and mobile devices. This includes setting up standard configurations, installing necessary software.
R4.2	Experience of providing training and support to end-users during the rollout process. This could involve conducting training sessions, creating user documentation, and addressing user questions and concerns.
R4.3	Experience of preparing laptops and mobile phone hardware for roll-out to large number of users.
R4.4	Experience of 1st/2nd line ServiceDesk/desktop support in a Windows environment
R4.5	Active Directory user and computer administration
R4.6	Experience of using ITSM tools for service management
R4.7	Experience of working on large roll-out projects within an IT environment
R4.8	Excellent communication skills with the ability to interact with staff at all levels of the organisation.
R4.9	Good knowledge of Microsoft office 365 applications
R5.1	Unbox and prepare the devices for deployment. This includes activities such as installing operating systems, configuring network settings, applying security settings, and installing necessary software and applications.
R5.2	If applicable, transfer data and user settings from the old devices to the new ones. This can be done through various methods such as data backups, cloud synchronization, or manual transfer.
R5.3	To ensure user adapt to new devices and services quickly to minimise disruption, provision of training sessions to familiarise users with the new devices and any changes in software.
R5.4	Distribute the new devices to the associated users. This will involve physically handing over the devices, configuring user accounts, and assisting users with initial setup.
R5.5	Update the inventory and asset management systems to reflect the new devices and retire the old ones.



Ref	Requirement
R5.6	<p>CMA has around 1000 staff across all sites and has offices in London Headquarters - Canary Wharf, where most of our staff are based but also a significant presence in Scotland, as well as offices in Wales and Northern Ireland, Darlington and Manchester.</p> <p>The office breakdown and <u>approximate</u> increasing user numbers are as follows:</p> <ul style="list-style-type: none">• • • • • • <p>Delivery of these services will be to all CMA locations as and when required.</p>

3. GENERAL DATA PROTECTION REGULATION (GDPR)

- 3.1. All system configurations will be on the CMA network. The supplier will be given access to the CMA's Azure test environments during development via secure login.
- 3.2. No data shall be copied from the CMA network.

4. PAYMENTS

- 4.1. The Supplier should propose a payment regime noting the following:
 - The CMA cannot pay for services in advance of receipt of services.
 - Setup should be associated with delivery milestones.
- 4.2. Payments shall be monthly in arrears. The CMA shall pay within 30 days of having received a valid invoice. All invoices must quote a Purchase Order (PO) number and set out a description of the services and deliverables provided during that invoicing period. Invoices should also provide a breakdown of the costs which align with the contracted rates/sums and quote the CMA Contract Manager.
- 4.3. Invoices will be determined to be invalid if any of the details in 9.2 is missing.

5. CONTRACT PERIOD

- 5.1. Optional extensions will be subject to agreement on scope of services required in each subsequent extension option. Where an extension is agreed the scope of the



services will be agreed (i.e. year 3 may only require 1x Service desk resource and year 4 may only require EUC rollout engineers).

6. CONTRACT MANAGEMENT and REVIEW ARRANGEMENT

6.1. The Supplier shall:

- appoint a suitably experienced and dedicated account Lead. The Project Lead shall act as the main point of contact for all administrative arrangements, queries and issues. In addition, the Project Lead will be responsible for overseeing the entire engagement, coordinating with our internal teams, and providing regular updates on project progress to CMA manager as required.
- Submit performance reports (at least monthly) for review by the CMA.
- Ensure that replacement of personnel of the same or higher calibre are provided to the CMA should any Key Personal be absent for whatever reason and within one day (or as otherwise agreed with the CMA) of that absence occurring.
- have a clear escalation process for any project-related issues. They should promptly address and resolve any problems that may arise during the project execution and escalate to senior management if required.

6.2. This contract has an option for project rollout resources where the following should be noted:

- CMA will send the supplier an email outlining their requirements for any future project streams which the CMA wish the supplier to take on, under this contract.
- The supplier will meet with the CMA Contract Manager and Project Manager and discuss this requirement.
- The supplier will then submit a Proposed Statement of Work (SoW) setting out:
 - An approach and methodology for meeting the requirements
 - A Project Plan identifying key resources to be utilised, number of days, key milestones/deliverables and dates; and
 - A full breakdown of costs.
- The CMA will review the Proposal and where appropriate, ask the Contractor to clarify any aspect of their Proposal and re submit an amended Proposal.
- If the CMA agrees to proceed with the Proposal, it shall sign the SoW and additionally issue a Purchase Order (PO) referencing the Proposal to the Contractor under the terms of the existing contract.
- Formally then a contract variation will be done using the corresponding process detailed in the contract.
- The CMA reserves the right to not proceed with any SoW and to source the services from an alternative route.



7. KEY DATES

7.1. The following dates are to apply to this service:

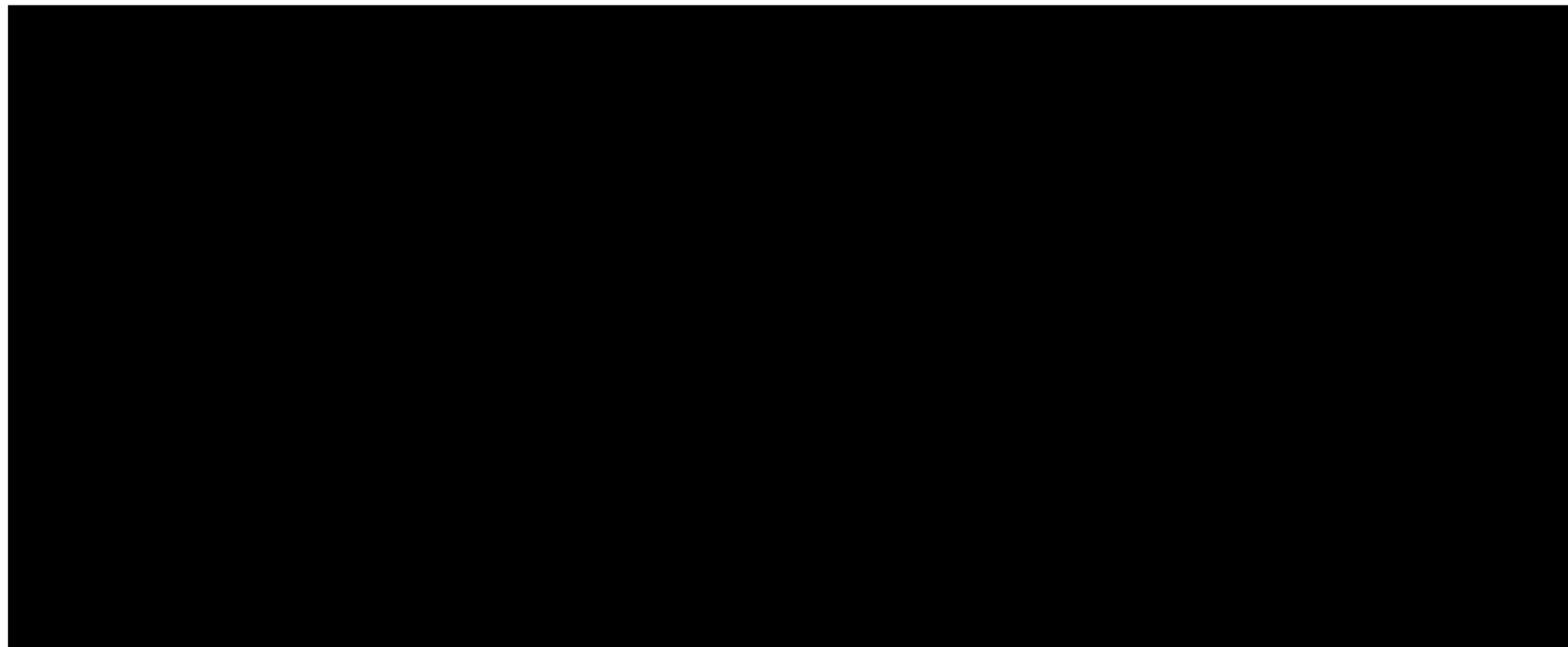
Milestone	Detail	Service	Date
M1	Milestone whereby the new service is to start (Service Commencement date).	Service Desk Support	Contract Start Date: 01/04/24
M2	Timeline estimates for EUC project	EUC Project	2 months following M1
M3	Annual service review.	Service Desk Support	12 months after service commencement (M1 + 12 months)



Crown
Commercial
Service

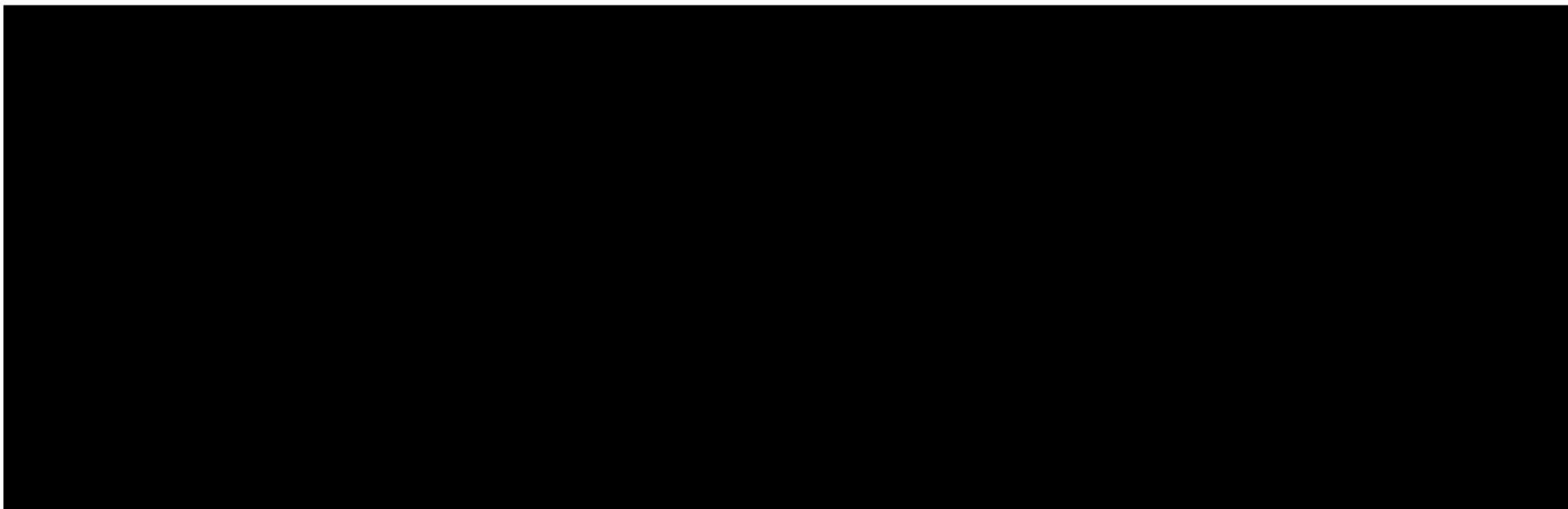
Attachment 2 – Charges and Invoicing

Core Services

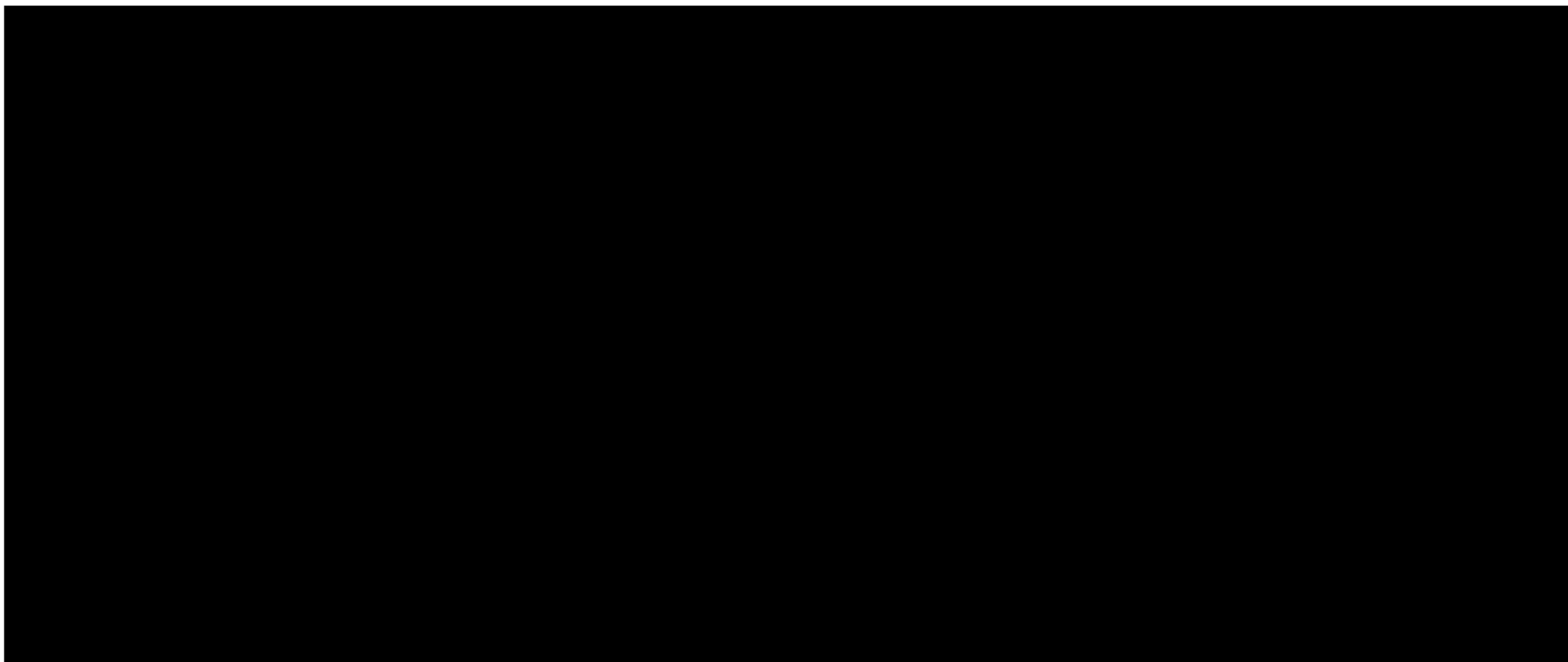




Crown
Commercial
Service

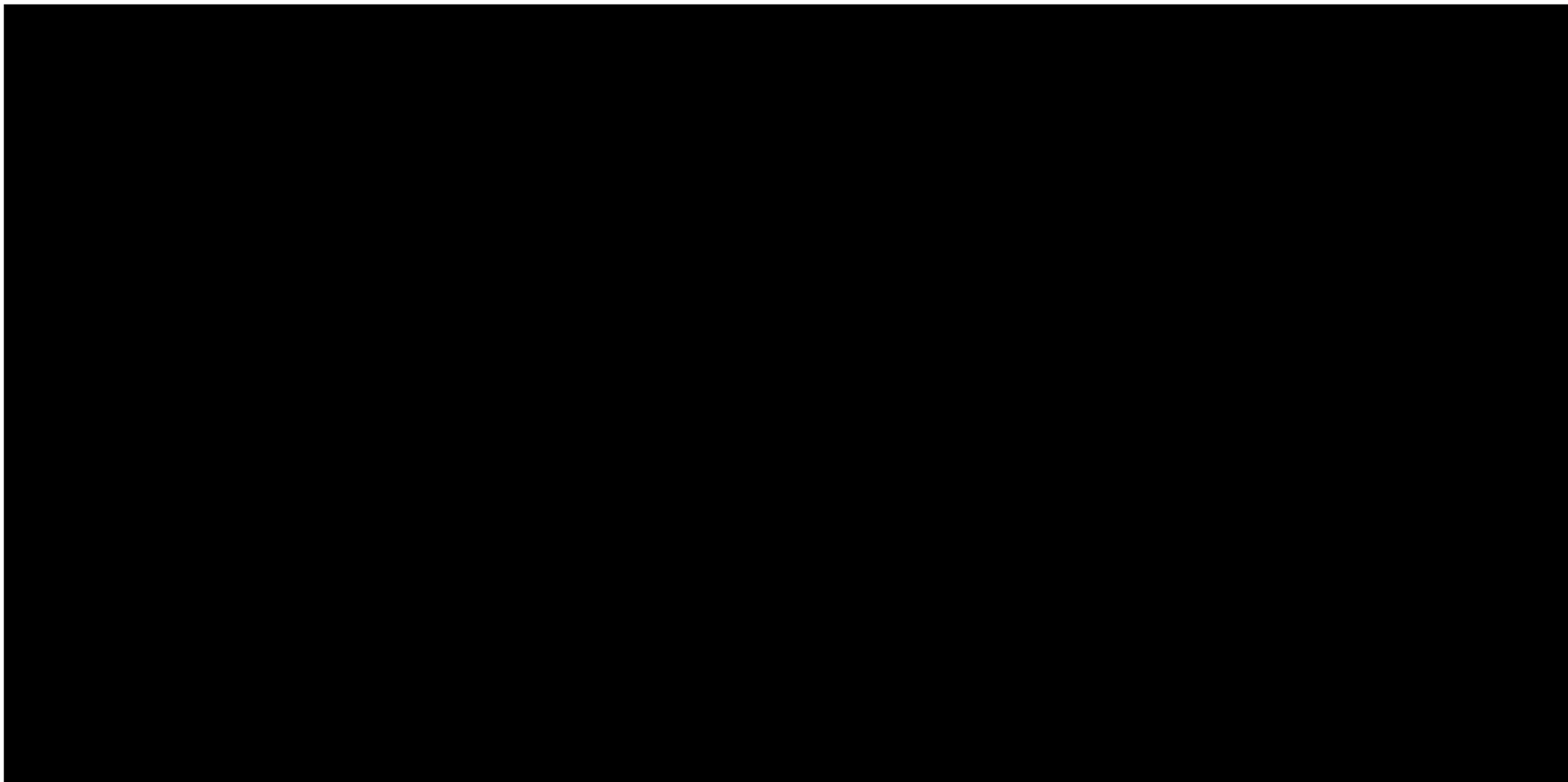


Optional Services





Crown
Commercial
Service



Early Termination Fee(s)

Any outstanding fees incurred from delivered services to the buyer up until the termination date.



Attachment 3 - Supplier Clarifications

1. The Supplier confirms it understands all clarifications provided by The Buyer in Appendix 3 - ICT Operational Services ITT clarifications” and that the Supplier’s bid was made in accordance with this information.



Attachment 4 – Service Levels and Service Credits

Critical Service Level Failure

In relation to the Supplier resource's performance, a Critical Service Level Failure shall include a delay in producing a response or resolution of incidents assigned by the Buyer in excess of a weeks' notice, more than once in any quarter, or more than 4 times per year.

In relation to quality of Supplier resource a Critical Service Level Failure shall include a delay in Supplier resource producing a service in line with the CMA SLA levels assigned by the Buyer in excess of a month, or more than once in any 2-month period.

In relation to Supplier Communication a Critical Service Level Failure shall include a delay in the Supplier producing IT support services assigned by the Buyer in excess of a 2 week period, more than once in any in any month.

In relation to the Supplier replacing their resource(s) a Critical Service Level Failure shall include a delay in producing alternative IT support resource ordered by the Customer in excess of 1-week, more than once in any quarter.



Attachment 5 – Key Supplier Personnel and Key Sub-Contractors

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
		<i>Contract Period</i>
		<i>Contract Period</i>
		<i>Contract Period</i>

Part B – Key Sub-Contractors

N/A

Attachment 6 – Software

N/A

Attachment 7 – Financial Distress

For the purpose of Schedule 7 (Financial Distress) of the Call-Off Terms, the following shall apply:


PART A – CREDIT RATING THRESHOLD

Entity	Credit Rating (long term) <i>(insert credit rating issued for the entity at the Commencement Date)</i>	Credit Rating Threshold <i>(insert the actual rating (e.g. AA-) or the Credit Rating Level (e.g. Credit Rating Level 3))</i>
Supplier	Dun & Bradstreet Failure Score – 94	Dun & Bradstreet Failure Score – 30

Attachment 8 – Governance

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	
Supplier Members for the Operational Board	
Frequency of the Operational Board	Monthly – Unless stated otherwise by The Buyer
Location of the Operational Board	Online meeting or in-person. This will be arranged by The Buyer prior to the meeting. In-person meetings could take place in any of the aforementioned Buyer Premises

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. The contact details of the Buyer's Data Protection Officer are: [REDACTED]
2. The contact details of the Supplier's Data Protection Officer are: [REDACTED]
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
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 Authority is Controller and the Supplier is 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> <ul style="list-style-type: none"> Conduct contractual deliverable(s), detailed within the Statement of Requirements and manage the contract
Duration of the processing	The length of the contract deliverables
Nature and purposes of the processing	The nature of the Processing will be to consult with CMA staff on work related matters to inform the contract outputs.
Type of Personal Data	First name, second name, phone number, home address details, employee number, grade, possible health related issues in relation to occupational health referrals for specialist hardware or software.
Categories of Data Subject	CMA Staff

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	Up to 3 months following the end of the contract.
--	---

Attachment 10 – Transparency Reports

Title	Content	Format	Frequency
Call-Off Contract	Burndown report of services used	Excel	Monthly
Charges	Burndown report of services used	Excel	Monthly

Appendix 1 – ICT Acceptable Use and Access Control Policy



ICT ACCEPTABLE USE AND ACCESS CONTROL POLICY

Version – v1.04
Release Date - May 2023

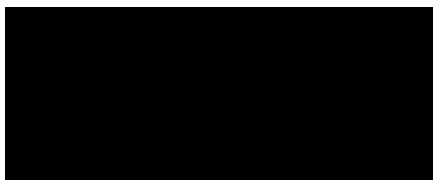
FOREWORD

The information held by the Competition and Markets Authority (CMA) is valuable, especially information relating to an inquiry, competition law investigation, consumer law investigation, or appeal.

Measures need to be taken to protect this information from breaches of security, not only to comply with our legal and contractual obligations, but also to retain a high degree of trust amongst the public and business community. This trust is essential to the effective operation of the CMA. The CMA provides appropriate protection for its information and other assets in accordance with the principles of risk management, and in line with Cabinet Office advice and HMG Security Policy Framework (SPF).

The protection of information is the responsibility of everyone within the CMA, CMA Members, non-executive directors, board members, secondees, temporary staff, contractors, and in some cases third party suppliers, all who may have access to CMA ICT systems and other information held by the CMA.

Everyone should therefore familiarise themselves and comply with this policy and other associated security policies and procedures.



1 Purpose

1.1 This policy applies to all users (including CMA staff, CMA Panel Members, nonexecutive directors, board members, secondees, parental leave, temporary staff, contractors and in some cases third party suppliers). It describes the responsibilities and rights of all who are given access to the CMA's information assets, information systems and communications devices. Information assets and information systems include such things as email, secure email, and the internet (including blogs and other means of information publication). Communication devices include mobile phones, laptops, tablets, stand-alone terminals, remote working solutions, audio, and video devices.

1.2 Access and use of the CMA's information assets, information systems and communications devices is provided for business use. Employees are accountable for the way that these resources are used and the purposes that they are intended. This document sets the minimum requirements for staff use.

It confers certain privileges on employees and details their responsibilities in relation to both official and personal use of CMA resources.

1.3 Information is an asset which has value and needs to be protected. Much of the information held by the CMA has been obtained under statutory provisions which require that it shall not be disclosed without consent. The protection of information held by the CMA is critical to meeting its contractual and legal obligations, as well as credibility in the eyes of the public and the business community.

1.4 Information security measures are necessary to protect information from a wide range of threats. Information security comprises the preservation of:

- Confidentiality: ensuring that information is accessible only to those authorised to have access;
- Integrity: safeguarding the accuracy and completeness of information and processing methods; and
- Availability: ensuring that authorised users have access to information and associated assets when required.

2 Roles & Responsibilities

2.1 Each designated system owner is responsible for:

- The ownership, management, control, and security of the information processed on behalf of the CMA.
- Making sure adequate procedures are implemented so as to ensure all CMA employees, third parties and others that report to them are made aware of and are instructed to comply with this policy and all other relevant policies.
- Making sure adequate procedures are implemented to ensure compliance of this policy and all other relevant policies.
- Ensuring adequate backup procedures are in place for the information system they are responsible for.
- Ensuring all access requests are evaluated based on the approved criteria.
- Designating the system administrator(s).
- Providing the system administrator(s) with a list of nominees who are authorised to approve and sign access requests to the system on their behalf.
- Informing TBS and DPO immediately in the event of a security incident involving the systems they are responsible for.

2.2 Each system administrator is responsible for:

- Complying with the terms of this policy and all other relevant CMA policies, procedures, regulations, and applicable legislation.
- Taking prompt action on receipt of requests for user registration, change of privileges, password resets and de-registration of users in accordance with this policy.
- Taking appropriate and prompt action on receipt of requests for the suspension of a user account in accordance with this policy.
- Ensuring all passwords generated for new user accounts and password resets meet the requirements of the CMA policies
- Notifying users of their system account details in a secure and confidential manner.
- Ensuring that records of all authorized user registrations, change of privileges and de- registration requests are maintained and made available for review to
the appropriate personnel, Informing TBS immediately in the event of a security incident.
- Complying with instructions issued by TBS on behalf of the CMA.

2.3 TBS is responsible for:

- The management, control, ownership, security, and integrity of all CMA network on behalf of the CMA.
- The implementation of this policy and all other relevant policies within TBS.
- Ensuring adequate procedures are in place to ensure compliance with this policy and all other relevant policies.

2.4 Each Line Manager is responsible for:

- The implementation of this policy and all other relevant CMA policies within their teams.
- Ensuring that all people who report to them are made aware of and are instructed to comply with this policy and all other relevant CMA policies.

- Ensuring complete and timely user access requests, for both permanent and temporary staff, are forwarded to the designated system owner allowing sufficient time for the creation of the required user account prior to the users start date.
- Ensuring complete and timely user network access requests for people are forwarded to TBS allowing sufficient time for the creation of the required user account prior to the users start date.
- Ensuring that each user they request access fulfils all the criteria (principle of “least privilege”) for the requested system.
- Ensuring they make timely requests for the suspension of all user accounts belonging to members of their staff who are taking a career break, going on maternity leave or leave or those on long term sick leave.
- Ensuring they make timely requests for the deletion of all user accounts belonging to people who are leaving the employment of the CMA.

2.5 Each user is responsible for:

- Complying with the terms of this policy and all other relevant CMA policies, procedures, regulations, and applicable legislation.
- Respecting and protecting the privacy and confidentiality of the systems they access, and the information processed by those systems.
- Ensuring they only use user access accounts and passwords which have been assigned to them.
- Ensuring all passwords assigned to them are kept confidential at all times and not shared with others including their co-workers or third parties.
- Changing their passwords when instructed to do so by system administrators, network administrators or TBS.
- Complying with instructions issued by designated information owners, system administrators, network administrators and/or TBS on behalf of the CMA.
- Reporting all misuse and breaches of this policy to their line manager.

3 General Acceptable Use Standards

3.1 Use of CMA ICT Infrastructure

3.1.1 The CMA's information assets and ICT infrastructure are to be used solely for the purposes for which the computer access was intended.

3.1.2 It is not acceptable to use the ICT Infrastructure to create, send, access or store information that:

- could damage the reputation or financial position of the CMA.
- involves or could lead to victimisation, discrimination, harassment, or vilification.
- is sexually suggestive, offensive, obscene, threatening, abusive, defamatory, fraudulent, unauthorised, deliberately misleading, or deceptive, unless it is part of legitimate CMA business.
- is used for operating a private business not related to the CMA's operations.
- is encrypted or password protected without approval or without providing effective recovery of the encryption passphrases or keys.
- violates any law (e.g., data protection, copyright, and crime laws).
- may hinder productivity within the CMA such as writing, sending, or forwarding chain mails (those that, in the body or subject of the message, asks the recipient to forward the email on to multiple people. Many are hoaxes and are often considered to be a security and privacy risk to collect valid lists of email addresses.) streaming private videos, or sharing private files; or
- may damage or impair any other ICT systems (such as sending malware or intentionally initiating a denial of service on any ICT system).

3.1.3 Inappropriate or unacceptable material must not be accessed or stored at the CMA premises or on its computers (including PCs, laptops, Mobile phones, and tablets), unless it is part of legitimate CMA business.

3.1.4. The CMA may investigate, replicate, or remove any illegal or unacceptable material from its sites and computers without notice.

3.1.5 Instances of criminal or inappropriate activity must immediately be reported to management in accordance with the CMA security incident reporting procedure.

3.1.6 Private use is permitted but must be kept to a minimum, as described in [Section 8 - Private Use of ICT Infrastructure](#).

5.

3.2 Access to Information and Information Systems

3.2.1 Users shall use their own log-in account and shall not use any other person's log-in account, either with or without their permission.

3.2.2 All users must protect their passwords/PINS from unauthorised use and are responsible for all activities associated with their User ID.

3.2.3 Users shall not intentionally attempt to gain unauthorised access to, cause damage to, or alter CMA systems and software. This includes, but is not limited to, performing unauthorised modification of operating systems, or configuration files.

3.2.4 Users shall not intentionally alter or avoid any systems auditing, logging or other security and control mechanisms.

6. 3.3 Access during Absences

3.3.1 Any access request to a mailbox belonging to a user on absence, must be approved by the Chief Operating Officer (COO) or his deputy, the Senior Director, People, Capability and Culture (SD(PCC)). Delegate access is issued once approval is granted. This access remains active for period of time approved, after which it is revoked.

3.3.2 In the absence of a user who has not given delegate access to their ICT, any delegate access required for business reasons must be supported by the line manager or the

Inquiry/ Project Director on the relevant inquiry or project, and Technology and Business Services (TBS) must be informed. Authorisation will be needed from the COO or SD(PCC), for access to be granted. Once the user has returned, any delegated access must be removed.

3.3.3 Executives, managers, and staff in critical positions should establish appropriate 'delegates' to perform actions in their absence. For example, the absence of a system administrator should not stop work on a computing system.

3.3.4 When staff leave the CMA, their account will be disabled in the evening of their last working day. User accounts are deleted no earlier than three months after their last working day. This does not apply when there is a reasonable prospect that data in an account may be relevant to any dispute (either with the staff member or otherwise) where litigation may arise. In those circumstances, the Line Manager of the user leaving must inform HR if they wish for their account to remain archived for any reason (e.g., for a possible employment tribunal claim by the staff member). HR must forward this request to the ServiceDesk (TBS) and copy the request to the Departmental Security Officer (DSO).

3.3.5 Staff taking maternity, adoption or shared parental leave will typically return all CMA equipment and be configured to use Windows Virtual Desktop (WVD) which permits the use of a personal home device. Staff who do not have a personal home device that they can use will have the option to retain their CMA laptop (and phone). The request to retain CMA equipment under any other form of absence (e.g. career break, unpaid special leave lasting longer than four weeks) will require authorisation from the COO or SD(PCC).

3.4 Emergency Access during Absences

3.4.1 In emergency situations where access to an absent person's files or email is essential, approval must be obtained from the COO or SD(PCC) and documented prior to using the person's account.

3.5 Software Copyright and Licences

3.5.1 ICT administrators shall only use legal versions of licensed software in compliance with vendor licence requirements. Software may only be copied as stipulated in the licence agreement.

3.6 ICT Resources and Network Connectivity

3.6.1 Users must not remove computer equipment, software, illicitly modify files (this excludes collaboration projects where the file owner has shared a file and has invited other users to make changes), passwords/PINS or any data belonging to another user (where the user believes they have an expectation of privacy e.g.

a file on OneDrive until the user shares it), unless authorised by the COO or SD(PCC).

3.6.2 When connected to the CMA network, users must not:

- tamper with security systems.
- probe for system or network information or vulnerabilities.
- attempt to exploit a potential security vulnerability; or
- try to access any systems without authority.

4 Laptop and Office Security

4.1 When leaving a desk unattended, users must lock their laptop using “ctrl + alt + delete” or “Windows + L” shortcut. The session will be automatically locked after 10 minutes, if using the battery, or 15 minutes of inactivity if connected to the mains. If equipment is left unlocked, the user may be responsible for any activity that takes place.

4.2 When leaving a laptop for an extended period, users should log off.

4.3 When leaving the office at the end of the day, users should shut/power down their device before storage.

5 User Accounts and Passwords/PINS

5.1 User Accounts

5.1.1 Individuals are accountable for all actions performed under their account on CMA systems.

5.2 Managing Passwords/PINS

5.2.1 Password/PIN security is an important safeguard that guarantees the integrity and confidentiality of data.

5.2.2 Passwords/PINS must not be reused (they must be unique), shared, based on anything somebody else could easily guess or obtain using person related information (e.g. names, telephone numbers and dates of birth).

5.2.3 Your CMA mobile phone password/PIN must also be at least 7 characters in length. It must include a mixture of upper- and lower-case letters, a symbol and a number.'

5.2.4 If you cannot remember a password/PIN, contact the ServiceDesk who will assist with the reset and creation of a new one.

5.2.5 If you suspect your password has been compromised, you must report this to the Service Desk immediately. If your password has been compromised and you do not act, you may be held accountable for actions taken under your username.

5.2.6 CMA staff should not use the same password/PIN for CMA internal systems and external non-CMA systems. External system passwords/PINS may easily become compromised and that may permit compromise of a CMA system.

5.2.7 Do not use the same password/PIN across different ICT devices (e.g., Phone and tablet).

5.3 Windows Hello for Business

5.3.1 You must set up Windows Hello for Business on your laptop. You may access your laptop using a user-id and password initially when you receive your laptop, but you must set up Windows Hello for Business.

5.3.2 Windows Hello for Business biometric face recognition or fingerprint access is the simplest and quickest way to access your laptop that is favoured by the organisation. However, some people may not be comfortable using the biometric access. Where that is the case, you will be required to use a PIN that you will need to set up.

5.3.3 If you need help setting up Windows Hello for Business, please contact the Service Desk.

5.4 Privileged Accounts

5.4.1 Any person who uses a privileged system or service account (e.g., an ICT administrator) must not use that account when a less-privileged account would suffice.

5.4.2 When privileges are required, users should switch to a privileged account to ensure that an audit trail is maintained.

5.4.3 Before privileges can be assigned to user's accounts, the users must have management approval and a valid business reason. Privileged accounts must be regularly revalidated.

6 Principles of Access Control

6.1 All ICT resources must have appropriate authentication controls using Multi Factor Authentication (MFA).

6.2 Each CMA system must have a designated owner who is responsible for managing and controlling access to the system.

6.3 Each CMA system must have designated system administrators who are responsible for the day-to-day administration of the system including the creation and management of system access accounts for authorised users. Some information systems may, for historical reasons, be directly managed by TBS who will perform the role of system administrator.

6.4 TBS is the designated owner of the CMA network domain. Network administrators are responsible for the day-to-day administration of the network domain, including the management of accounts for authorised users.

6.5 Access to the CMA network must be strictly controlled by a formal registration and de-registration process.

6.6 Access to CMA systems must be controlled using individual user access accounts.

The use of generic or group access accounts to gain access is prohibited.

7 Account Registration

7.1 CMA Staff Access Accounts

7.1.1 Access to CMA Systems will be controlled via individual user access accounts. This will be, initially, userid and password and then Windows Hello for Business. The creation and/or use of generic accounts is not permitted under any circumstances on CMA information systems (except where system or service accounts are needed).

7.1.2 All new requests for access to information systems must be made via the ServiceDesk Portal and will follow standard ServiceDesk request procedures.

7.1.3 Line managers must complete the request on behalf of a new user and send this onto the designated information owner or their nominee for their approval.

7.1.4 System owners or their nominees must formally authorise and sign all new access requests. Once a request for access has been approved, the system owner or their nominee must sign the system access request and forward this onto the system administrator for the user account to be created.

7.1.5 System administrators must only create new user accounts when they have received a valid system access request.

7.1.6 User access accounts must be created so they clearly identify users so that audit trails and logs do not become obscured.

7.2 Third Party Access Accounts

7.2.1 Where there is a business need, and with the approval of a CMA system owner or their nominee, a third-party service provider may be granted access to the CMA network and systems.

7.2.2 Third party commercial service provider access requests must be sponsored by a CMA system owner or their nominee and submitted to TBS in writing.

7.2.3 Under no circumstances will third party service providers be granted access to the CMA network and information systems until TBS has received the proper authorisations.

7.2.4 Third party service provider access privileges will be agreed on a case-by-case basis. The third-party service provider must liaise with the CMA to establish the connections may be set up on a more permanent basis for ongoing information system or network support purposes.

7.3 User Account Management

7.3.1 Requests from users for password/PIN resets must only be performed once the user's identity has been verified by the appropriate system administrator or network administrator.

7.3.2 Existing users who require additional access privileges on a system must obtain the written authorization of the designated system owner or their nominee. In accordance with this policy, line managers must initiate the requests using the CMA System Access Request procedure.

7.3.3 The access accounts of users who are about to change roles or transfer to another CMA directorate or service area, must be reviewed to ensure access account privileges that are no longer required by the user in their new role are removed. In such circumstances the user's existing line manager must request the removal of the unnecessary account privileges. The request must be made in writing using the minimum privileges required by them for them to complete the service they have been contracted to perform.

7.3.4 Local access (on-site) to the CMA network and information systems may be granted on a temporary basis only as and when the need arises. Remote access

7.3.5 CMA Suspend / Remove Access procedures and forwarded to TBS or the appropriate system administrator before the user changes role or transfers.

8 Account De-Registration

8.1 User accounts for those leaving the employment of CMA are terminated on the last working day. This is indicated in the Leaver Notification form generated by HR. Line managers must notify HR when informed by users of their wish to leave CMA employment.

8.2 System administrators and network administrators must revoke user access and disable accounts at the requested date and time after the receipt of a leavers notification being generated by the HR team.

9 Private Use of ICT Infrastructure

9.1 All users are permitted to use CMA-provided email, communications devices, and Internet for reasonable private use.

9.2 The downloading of games, music, movies, and image files for private or illegal use on CMA equipment is prohibited.

9.3 CMA systems must not be used to circulate programs or other material, including 'chain letters' (a message that asks the recipient to pass the email on to a certain number of recipients in an exponentially growing pyramid).

9.4 Any private use must not impact on the CMA's service delivery, incur excessive costs, or create an exposure to malware, legal liability, or embarrassment.

9.5 All usage of the ICT infrastructure is recorded and may be monitored and reviewed.

10 Virus Protection

10.1 Viruses or Malware are forms of malicious software which are unknowingly activated by a user. It can have several effects ranging from the denial of service to the destruction of data.

10.2 Use of the Internet and the sharing information using magnetic media or email, increases the threat of a virus attack.

10.3 The CMA has anti-virus software installed on all servers and laptops which is kept up to date.

10.4 To minimise the risk of virus infection:

- Do not use any unofficial or unauthorised software on your laptop;
- Contact the Service desk if you think that an email is a phishing attempt. Do not open it;
- Never boot your machine from a USB device;
- Notify the Service Desk If you receive a virus alert from outside the CMA; and
- Contact the Service desk if you think your CMA device may have picked up a virus.

10.5 Everyone who has a CMA device should check at least weekly to see if there are any updates to be applied. Updates should be applied immediately. Using a device without implementing an update when one available, exposes it to known malware.

11 Email

11.1 General

11.1.1 CMA email is available for communication on matters directly concerned with the business of the CMA. It is, however, recognized that as a member of staff, you may wish to use electronic mail for personal matters. This is acceptable; however, you should remember that it is a privilege and if the privilege is abused, you may be subject to disciplinary action. Personal use of the email system must be moderate, reasonable, and appropriate, and it must not interfere with your work.

11.1.2 The CMA expects staff to behave responsibly when they use the email system. Under no circumstances should the use of personal email be allowed to adversely affect your work performance (or disrupt that of others). Nor must

your activities affect the overall performance of the ICT system (for example, by downloading or sending large files or programs; or those with a high risk of virus contamination). You must not send abusive, offensive, demeaning, or malicious messages. This includes, but is not limited to, messages inconsistent with the CMA's Bullying and Harassment Policy.

11.1.3 The following are examples of acts of misconduct which are prohibited and may lead to disciplinary action, as per the CMA's Disciplinary Policy:

- Sending abusive, bullying, offensive, demeaning, or malicious messages.
- Sending a message that could constitute harassment (on the grounds of sex, marital status, religion, race, colour, nationality, ethnic origins, national origins, age, sexual orientation, or disability).
- Sending, knowingly receiving, viewing, or displaying sexually explicit or pornographic material (images and writing).
- Sending chain letters.
- Disclosing confidential information without lawful authority.
- The distribution of any unauthorized software.
- Sending unencrypted OFFICIAL SENSITIVE material by external email (outside the CMA). Please contact the Security Team if you need any advice on what is considered OFFICIAL SENSITIVE or encryption.
- Sending any material above OFFICIAL-SENSITIVE by email.
- Using the email system to solicit or conduct business other than the business of the CMA.
- Accessing colleagues' email accounts without their prior consent.

11.1.4 These examples are illustrative and do not constitute an exhaustive list.

11.2 Spam Mail

11.2.1 Unsolicited or unwanted emails are referred to as Spam. The CMA uses email filtering technology to minimise the receipt of Spam emails. If you receive Spam mail, you should immediately delete it and do not respond. All such incidents must be raised with the Service Desk

11.2.2 Spammers use automated systems to search on-line for email addresses. When publishing your email address on the internet, protect it by using your name hyperlinked to your email address. This will reduce the likelihood of receiving spam.

11.3 All Staff email (Broadcast Emails)

11.3.1 Approval should be obtained from the Internal Communications team before sending “All Staff” emails. The Weekly Brief is the preferred medium for broadcasting information directed to all staff.

11.4 Electronic Calendars

11.4.1 Users must ensure that their Outlook Calendar can only be viewed by appropriate persons within the organisation or by invitation.

11.4.2 Be careful attaching documents in meeting invites, as this may disclose sensitive or private information to other people able to see your calendar.

12 Telephone

12.1 Occasional personal use of office telephones is acceptable. Calls should be as brief as possible and within the UK. A record is kept of the length of all calls and the recipient’s number. These will be provided by the Director of TBS to a Line Manager who is concerned about a user’s performance, or to help the progress of an investigation into misconduct or criminal activity.

12.2 Staff should be aware of telephone techniques used to manipulate them to carry out actions or divulge confidential information (social engineering). The telephone can be used as a method to unlawfully gain classified information (e.g., by pretending to be from another part of the organisation and asking for an update on a case or project). To mitigate this risk, avoid giving out classified information over the telephone, especially personal details of an individual. If you are unsure about a caller, you should take their name and number and telephone them back, having taken steps to confirm their identity.

13 Internet

13.1 General Use

13.1.1 Personal use of the Internet must not adversely affect your work performance or the overall performance of the ICT system (e.g., downloading large files or programs with a high risk of malware contamination).

13.1.2 The following are illustrative examples (and not exhaustive) of acts of misconduct which are prohibited and may lead to disciplinary action (if not part of CMA legitimate business), as per the CMA’s disciplinary policy:

- Visiting inappropriate sites, active downloading of material from such sites or the use of search criteria which are clearly intended to identify inappropriate material.
- Purchasing, sending, viewing, accessing, downloading, or displaying sexually explicit or pornographic material (images and writing).

- Store inappropriate material on any area of the CMA's Corporate ICT system, or removable media using the CMA's computer equipment.
- Purchasing, sending, viewing, accessing, downloading, or displaying any material which disparages others on the grounds of sex, marital status, religion, race, colour, nationality, ethnic origins, national origins, age, sexual orientation, or disability.
- Online gambling and computer games.
- Unauthorised downloading of software.
- Using the Internet to solicit or conduct business other than the business of the CMA.

13.1.3 If you receive any downloaded material or accidentally access an Internet site with inappropriate material, you should report this to the Service Desk as soon as practicable.

13.1.4 Internet use can be monitored.

13.2 Web Publishing

13.2.1 Staff must ensure that web publications do not identify names or contact details unless there is an authorised reason to do so.

13.2.2 Users must not publish information that may allow unauthorised parties to access CMA systems or bypass security controls.

13.2.3 Content on websites must be authorised prior to publication, periodically reviewed to ensure currency, and removed or corrected when information is not current or is inaccurate.

13.3 Social Networking and Blogs

13.3.1 Social Networking websites (e.g., Facebook, Twitter) are a communication channel and must be managed in a similar way to other channels (e.g. email, chat, instant messaging).

13.3.2 Some users are permitted access to Facebook and Twitter for 'business use'.

13.3.3 Blogs must not disseminate confidential, private, or sensitive, information.

13.3.4 You must not discuss CMA's business over the Internet or in newsgroups unless the requirement has been specifically detailed in your job description.

14 Security Tools

14.1 Users must not use password cracking, scanning, traffic sniffing or other security assessment tools on the ICT infrastructure, unless officially sanctioned by either the COO or SD(PCC), or Director of TBS.

14.2 Where there is a valid business need for use of security/scanning tools on the network it must be approved by the Director of TBS / Head of Security.

14.3 The use of 7-Zip to encrypt documents is discouraged and should be used judiciously. This is because the password can easily be forgotten, and this can be problematic at a later date. Where it is used the password should be written down, put in a sealed envelope and details written on it of who sent it, date and time sent and who the recipient was. It should then be put in a safe.

15 Offsite Use of Information and Equipment

15.1 Security for Off-Site Equipment and Information

15.1.1 Reference should be made to the prevailing Policy for the Management of Requests to Work Overseas for Personal Reasons, should you wish to take ICT equipment abroad.

15.1.2 Special care must be taken off-site when accessing the CMA's network from a remote location. Laptops, phones, and tablets must be protected as well as documents.

15.1.3 Where possible, the level of security at the remote location should be equivalent to that for onsite equipment used for the same purpose. Users must take reasonable precautions to protect CMA equipment and information assets.

15.2 Connecting to the CMA Network

15.2.1 You may access CMA services from an airport, train or hotel. Access to CMA services will be safe because a VPN will connect you and provide end-to-end encryption. If you are visiting sites on the internet, please check for the padlock next to the URL web address in your browser. This will ensure there is an encrypted link. If you ever receive a message like, "Your connection is not private" or "Certificate is not issued by a trusted authority" do not proceed. Please contact the Service Desk immediately who will be able to help.

15.2.2 Only CMA approved methods of connecting to the CMA network from a remote location is allowed. Users must correctly identify themselves and authenticate using their password initially and then by their Windows Hello for Business (WHfB) credentials.

15.2.3 Users must protect information and physical assets to prevent someone else from accessing the CMA network using their identity.

15.3 Travelling with ICT Equipment

15.3.1 While travelling, keep all portable electronic devices (including laptops, phones, and tablets) and information assets secure always. Portable electronic devices should:

- Not be used in public places where the screen, or keyboard, is easily visible, especially when reading or entering classified information.
- Not be left in a car overnight. If laptops or phones must be left in a car, they should not be visible and must be locked away in the boot before you reach

your destination. If the contents of your boot are visible from the outside, you must keep the devices with you.

- Keep your CMA equipment with you when you are travelling. You should take care when putting your laptop through x-ray scanners at airports to ensure that it isn't damaged. Under no circumstances should you check in your CMA devices as hold baggage when travelling by air; and
- Keep safe from environmental hazards (e.g., extremes in temperature).

15.3.2 All portable electronic equipment (e.g., laptops, iPads, phones) must be charged or they run the risk of being confiscated at airports.

15.3.3 All device locations are monitored and recorded for audit. Any device detected as being outside of the UK without authorisation will be disabled without warning.

16 Lost or Stolen Equipment

16.1 Equipment Loss

16.1.1 If ICT equipment is lost, the Service Desk must be notified immediately on 0203 738 6300 and a [Security Incident Notification Form](#) must be filed within 24 hours and sent to the Head of Security.

16.2 Equipment Theft

16.2.1 In cases of theft, the Police must be informed, and a police crime report number reported back to the Service Desk. The Service Desk must be notified immediately on 0203 738 6300 and a [Security Incident Notification Form](#) must be filed within 24 hours and sent to the Head of Security.

16.3 Equipment Damage or Failure to Return

16.3.1 Losing, severely damaging ICT equipment or failure to notify the Service Desk of a loss may be considered a disciplinary offence. You must treat CMA equipment with the same care as if it were your own personal equipment. While it is recognised that accidents may happen, you should do all you reasonably can to prevent it from being damaged in any way or lost. You will be held liable for any act or omission (i.e., something you have not done) that leads to avoidable loss or damage.

16.3.2 Penalties could include full or part payment of the loss/damage and/or no future loan of equipment. If an employee leaves whilst in possession of ICT equipment, the CMA reserves the right to withhold salary and/or outstanding expenses to cover the cost of any loss or damage.

17 Printing

17.1 Printers must not be left unattended if sensitive information is being printed.

17.2 Unattended printing is permitted only if physical access controls prevent unauthorised persons entering the printing area or viewing the material being printed.

17.3 Using personal printers at home is not permitted, unless authorised by the COO or SD(PCC).

17.4 Care should be taken with home printing and the same level of control should be exercised as if printing in the office. Printed documents should be secured when not in use and disposed of in accordance with CMA standards.

18 Removeable Media

18.1 CD Writing and USB Storage Device

18.1.1 The use of removable media has been disabled as a baseline in line with CMA requirements to protect data.

18.1.2 If you receive information from a third party on disk or USB storage device, you must take it to the Service Desk who will scan the media for viruses before uploading to the appropriate folder on the system.

18.1.3 If there is a legitimate business reason for use of USB media, then this must be agreed on a case-by-case basis with the COO or SD(PCC), and either the DSO, Head of Security or Security Adviser and a suitable business case documented. The transfer of data to removable media will be carried out by TBS.

19 Reporting Data Security Incidents

19.1 All users should report suspected data security breaches to the Head of Security and their line manager. Where the breach includes personal data, this should also be reported to the Data Protection Officer (DPO).

19.2 Prompt reporting ensures that appropriate action can be taken in a timely manner and assists the CMA in assessing the effectiveness of controls used to protect CMA information and ICT Infrastructure. It also ensures that the mandatory reporting deadlines set by the Information Commissioner's Office can be met.

20 Monitoring & Review

20.1 System owners, SharePoint site owners or their nominees must continually monitor access to their systems. They must perform periodic reviews of the systems they are responsible for to ensure:

- That each user access account and the privileges assigned to that account are appropriate and relevant to that user's current role or function.

- That the information system and the information processed by the system is only accessed and used by authorized users for legitimate reasons.

20.2 System administrators and network administrators must conduct a system review at least once every quarter. Following the review, any user access accounts which have been inactive for 60 consecutive days or more must be suspended unless instructed otherwise by the user's line manager. Suspended user accounts which have not been reactivated within a 12-month period should be marked for deletion, unless instructed otherwise by the user's line manager.

21 Enforcement

21.1 The CMA reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. CMA staff, contractors, subcontractors, or agency staff who breach this policy may be subject to disciplinary action, including suspension and dismissal as provided for in the CMA disciplinary procedure.

21.2 Breaches of this policy by third-party service providers may lead to the withdrawal of CMA information technology resources to that third party commercial service provider and/or the cancellation of any contract(s) between the CMA and the third-party commercial service provider.

Appendix 2 – Tender Response



methods 
AN ALTEN COMPANY

PROC 732 - ICT Operational Support Services

Competition and Markets Authority

5th January 202

[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]

Stage 2 Quality Questions

7. Your Experience

1	<p>Please describe relevant experience where you have delivered 1st and 2nd line support services. In your response please:</p> <ul style="list-style-type: none">a) Explain the service your team provided for two different customersb) Include a table where you self-certify your compliance (full, partial or non-compliance) to the 'Experience' requirements in the Statement of Requirements document. <p>Please note the following:</p> <ul style="list-style-type: none">• The CMA reserve the right to speak to your customer reference for verification.• Your response should be in MS Word, Arial size 12 font and be limited to 4x A4 pages including images.	35%
---	--	-----

[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]

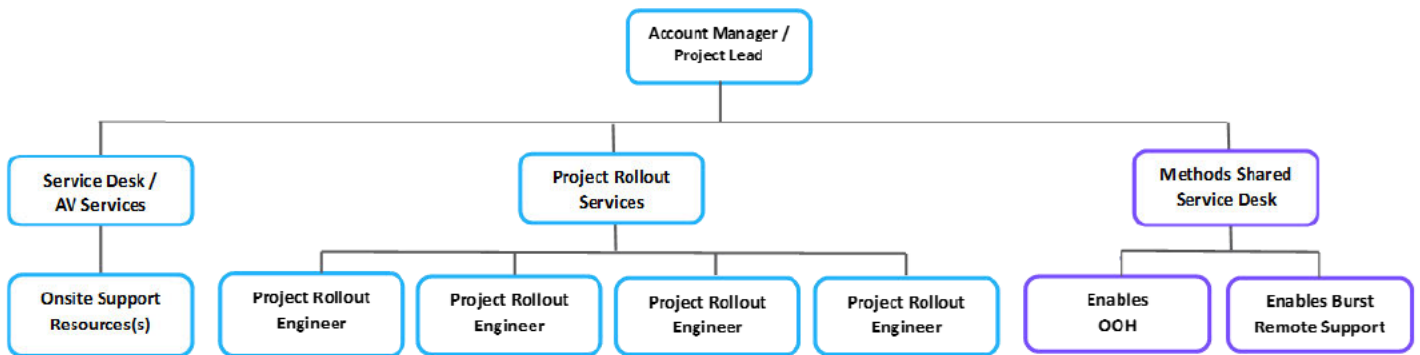
8. Your Proposed approach

2	<p>Please detail your company's understanding of the requirement and the arrangements you will put in place to ensure the quality of your service meets the CMA requirements including:</p> <ul style="list-style-type: none">a) Describe how you will meet the ServiceDesk/AV requirements.b) Describe how you will support EUC projects including associated processes to mobilise and manage resourcing.c) Any authority responsibilities. <p>Please note the following:</p> <ul style="list-style-type: none">• Your response should include a table where you self-certify your compliance (full, partial or non-compliance) to the 'General' requirements and the 'Task' requirements in the Statement of Requirements document.• Your response should be in MS Word, Arial size 12 font and be limited to 5x A4 pages including images.	30%
---	---	-----

[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted text block]

[Redacted text block]

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

		<div> <div></div> <div></div> </div>	

<div></div> <div></div> <div></div>	<div></div> <div></div> <div></div> <div></div>	<div></div> <div></div>
<div></div> <div></div> <div></div>	<div></div> <div></div> <div></div> <div></div> <div></div> <div></div>	<div></div> <div></div> <div></div> <div></div>
<div></div> <div></div> <div></div>	<div></div> <div></div> <div></div> <div></div> <div></div> <div></div>	<div></div> <div></div> <div></div> <div></div>
<div></div> <div></div> <div></div> <div></div> <div></div>	<div></div> <div></div> <div></div> <div></div> <div></div>	<div></div> <div></div> <div></div> <div></div>

-
-
-
-

[illegible]

Response	Percentage
Yes, the current administration is responsible	85%
No, the current administration is not responsible	15%

9. EUC Project

3	<p>Please demonstrate how you will support the CMA in a refresh project of 300 laptops and mobile phones. In your response, please detail:</p> <ol style="list-style-type: none">How you have supported other clients with a laptop and/or mobile phone refreshActivities your resources would doDescribe end user engagement in this project. <p>Please note the following:</p> <ul style="list-style-type: none">The CMA may seek to speak to any customer reference.Your response should be in MS Word, Arial size 12 font and be limited to 2x A4 pages including images.	30%
---	--	-----

[REDACTED]

[REDACTED]

Category	Sub-category	Value
Category 1	Sub-category 1	Value 1
Category 1	Sub-category 2	Value 2
Category 1	Sub-category 3	Value 3
Category 1	Sub-category 4	Value 4
Category 1	Sub-category 5	Value 5

[illegible]

		<ul style="list-style-type: none"> <ul style="list-style-type: none">
<ul style="list-style-type: none"> 	<ul style="list-style-type: none"> 	<ul style="list-style-type: none">

-
-
-

<ul style="list-style-type: none"> 	<ul style="list-style-type: none"> 	<ul style="list-style-type: none">
<ul style="list-style-type: none"> 	<ul style="list-style-type: none"> 	<ul style="list-style-type: none">

-
-
-
-
-
-
-

- -
 -
- -
 -
 -
- -
 -
 -

10. Out of Hours Support

4	<p>Please describe how you could deliver out-of-hour support services. In your response, please detail:</p> <ol style="list-style-type: none">When this support could be offeredThe nature of the support onsite or remoteThe resources required to support this kind of serviceAny customers that you already provide this type of service for <p>Please note the following:</p> <ul style="list-style-type: none">This is an optional service that the CMA is exploring, please cost this under the Optional Services in the Price ModelThe CMA may seek to speak to any customer reference.Your response should be in MS Word, Arial size 12 font and be limited to 2x A4 pages including images.	5%
---	---	----

[illegible]

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

[REDACTED]

Stage 3 Price Information

Service Change

[illegible][illegible]

[illegible][illegible]

Optional Services

</			

Additional Documentation

Please see attached:

Methods Case Study - Introduction and Maturity of the HMCTS DTS Service Desk

The attached case study is provided as an example of the impact and benefits of the Methods approach outlined in our overall response.

Stage 1 Compliance & Data Handling check

11. Supplier Information


Question number	Question	Your Response
1C.1(a)	Full name of the Person submitting the information	Methods Business and Digital Technology Limited
1C.1(b) – (i)	Registered office address (if applicable)	
1C.1(b) – (ii)	Registered website address (if applicable)	www.methods.co.uk
1C.1(c)	Trading status a) public limited company b) limited company c) limited liability partnership d) other partnership e) sole trader f) third sector g) other (please specify your trading status)	a) Limited company
1C.1(d)	Date of registration in country of origin	26 March 1990
1C.1(e)	Company registration number (if applicable)	
1C.1(f)	Charity registration number (if applicable)	N/A
1C.1(g)	Head office DUNS number (if applicable)	
1C.1(h)	Registered VAT number (if applicable)	
1C.1(i) - (i)	If applicable, is your organisation registered with the appropriate professional or trade register(s) in the member state where it is established?	N/A
1C.1(i) - (ii)	If you responded yes to 1.1(i) - (i), please provide the relevant details, including the registration number(s).	
1C.1(j) - (i)	Is it a legal requirement in the state where you are established for you to possess a particular authorisation, or be a member of a particular organisation in order to provide the services specified in this Procurement?	No
1C.1(j) - (ii)	If you responded yes to 1.1(j) - (i), please provide additional details of what is required and confirmation that you have complied with this.	

Question number	Question	Your Response
1C.1(k)	Trading name(s) that will be used if successful in this Procurement	
1C.1(l)	Relevant classifications (state whether you fall within one of these, and if so which one) Voluntary Community Social Enterprise (VCSE) Sheltered Workshop Public service mutual	N/A
1C.1(m)	Are you a Small, Medium or Micro Enterprise (SME) ¹ ?	No
<p>¹ See EU definition of SME https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en</p> <ul style="list-style-type: none"> I declare that to the best of my knowledge the answers submitted and information contained in this document are correct and accurate. I declare that, upon request and without delay I will provide the certificates or documentary evidence referred to in this document. I understand that the information will be used in the selection process to assess my organisation's suitability to be invited to participate further in this Procurement. I understand that the Authority may reject this Tender in its entirety if there is a failure to answer all the relevant questions fully, or if false/misleading information or content is provided in any section. <p>I am aware of the consequences of serious misrepresentation</p>		
Question number	Question	Your Response
1C.1(n)	Contact name	
1C.1(o)	Name of organisation	
1C.1(p)	Role in organisation	
1C.1(q)	Phone number	
1C.1(r)	E-mail address	
1C.1(s)	Postal address	
1C.1(t)	Signature	
1C.1(u)	Date	

Form of Agreement

FORM OF AGREEMENT	
Your Response	
To	The CMA, The Cabot, 25 Cabot Square, London E14 4QZ
Date	05/01/2024
<p>INVITATION TO TENDER PROC REF, PROC 732-2023</p> <p>I have examined the proposed Contract documents consisting of: Form of Agreement and Certificate of Bona Fide Tendering; Terms and Conditions of Contract; Statement of Requirement; Schedule of Rates and Prices; Tender Terms and Conditions and ITT Special Notices and Instructions to Tenderers.</p> <p>I hereby offer to enter into a Contract with the Authority upon the Conditions in the proposed Contract documents and for the Rates and Prices entered in the enclosed Schedule of Rates and Prices. Pricing information is valid for 90 days from the submission date.</p> <p>I warrant that I have all the requisite corporate authority to sign this tender.</p> <p>I have completed and appended the "Certificate of Bona Fide Tendering".</p> <p>I understand that the Authority is not bound to accept the lowest or any Tender.</p>	
Minimum Pass Mark:	Completion
Fail	Information supplied is missing or incomplete
Pass	Information supplied is complete
Name	<div></div> Date 05/01/24
Signature	<div></div>
Job Title	<div></div>
Duly authorised to sign Tenders on behalf of	<div></div>
Company Name	Methods Business and Digital Technology Limited

12. Certificate of Bona Fide Tendering

Certificate of Bona Fide Tendering				
<p>1. I declare that this is a bona fide Tender, intended to be competitive and that I have not fixed or adjusted the amount of the Tender by or under or in accordance with any agreement or arrangement with any other person ('person' includes any persons any body or association, corporate or incorporate) except as disclosed on this Certificate under 7 below.</p> <p>2. I declare that the Company is not aware of any connection with a member of the Authority's staff which could affect the outcome of the bidding process.</p> <p>3. I declare that I have not done and I undertake that I shall not do at any time any of the following:</p> <ul style="list-style-type: none"> a) communicate to any person, including the addressee calling for the Tender, the amount or approximate amount of the proposed Tender; b) enter into any agreement or arrangement with any other person or body that he or it shall refrain from tendering or as to the amount of any Tender to be submitted; c) enter into any agreement or arrangement with any other person or body that we shall refrain from tendering on a future occasion; d) offer or pay or agree to pay any sum of money or valuable consideration directly or indirectly to any person for doing or causing to be done in relation to any other tender for the Services any act of the kind described above; e) canvas or solicit the Authority's staff. <p>4. I understand that any instances of illegal cartels or market sharing arrangements suspected by the Authority shall be referred to the Competition and Markets Authority for investigation and may be subject to action under the Competition Act 1998.</p> <p>5. I understand that any misrepresentations may also be the subject of criminal investigation or used as a basis for civil action.</p> <p>6. In this Certificate "agreement" or "arrangement" includes any transaction private or open, or collusion, formal or informal, and whether or not legally binding.</p>				
Minimum Pass Mark:	Completion			
Fail	Information supplied is missing or incomplete			
Pass	Information supplied is complete			
Your Response				
Name			Date	05/01/2024
Signature				
Job Title				
on behalf of				
Company Name	Methods Business and Digital Technology Limited			

Information Security Terms and Conditions
<p><u>Security Conditions:</u></p> <p><u>Guidance for UK Contractors on the Protection of UK Assets marked as OFFICIAL - Sensitive</u></p> <p>1. The term "Authority" means the Contracting Authority.</p> <p>Security Grading</p> <p>2. The Authority shall issue a Security Aspects Letter which shall define the OFFICIAL - SENSITIVE information that is furnished to the Contractor, or which is to be developed by it, under this Contract. The Contractor shall mark all OFFICIAL - SENSITIVE documents which it originates or copies during the Contract clearly with the OFFICIAL - SENSITIVE classification.</p> <p>Official Secrets Acts</p> <p>3. The Contractor's attention is drawn to the provisions of the Official Secrets Acts 1911 to 1989 in general, and to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular. The Contractor shall take all reasonable steps to make sure that all individuals employed on any work in connection with the Contract (including sub-contractors) have notice that these statutory provisions, or any others provided by the Authority, apply to them and shall continue so to apply after the completion or earlier termination of the Contract.</p> <p>Protection of OFFICIAL - SENSITIVE Information</p> <p>4. The Contractor shall protect OFFICIAL - SENSITIVE information provided to it or generated by it in accordance with the requirements detailed in this Security Condition and any other conditions that may be specified by the Authority. The Contractor shall take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.</p> <p>5. OFFICIAL - SENSITIVE information shall be protected in a manner to avoid unauthorised access. The Contractor shall take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.</p> <p>6. All OFFICIAL - SENSITIVE material including documents, media and other material shall be physically secured to prevent unauthorised access. When not in use OFFICIAL - SENSITIVE documents/material shall be stored under lock and key.</p> <p>7. Disclosure of OFFICIAL - SENSITIVE information shall be strictly in accordance with the "need to know" principle. Except with the written consent of the Authority, the Contractor shall not disclose any of the classified aspects of the Contract detailed in the Security Aspects Letter other than to a person directly employed by the Contractor or sub-Contractor, or Service Provider.</p> <p>8. Any samples, patterns, specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the Contract remain the property of the Authority and shall be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 26.</p> <p>Access</p>

9. Access to OFFICIAL - SENSITIVE information shall be confined to those individuals who have a “need-to-know” and whose access is essential for the purpose of his or her duties.

10. The Contractor shall ensure that all individuals having access to OFFICIAL - SENSITIVE information have undergone basic recruitment checks. Contractors shall apply the requirements of HMG Baseline Personnel Security Standard (BPSS) for all individuals having access to OFFICIAL - SENSITIVE information. Further details and the full requirements of the BPSS can be found at the GOV.UK website at:
<https://www.gov.uk/government/publications/security-policy-framework>

Hard Copy Distribution of Information

11. OFFICIAL - SENSITIVE documents shall be distributed, both within and outside company premises, in such a way as to make sure that no unauthorised person has access. It may be sent by ordinary post or Commercial Couriers in a single envelope. The words OFFICIAL - SENSITIVE shall **not** appear on the envelope. The envelope should bear a stamp or details that clearly indicate the full address of the office from which it was sent.

Advice on the distribution of OFFICIAL - SENSITIVE documents abroad or any other general advice including the distribution of OFFICIAL - SENSITIVE hardware shall be sought from the Authority.

Electronic Communication, Telephony and Facsimile Services

12. OFFICIAL - SENSITIVE information shall normally be transmitted over the internet encrypted using a 256 AES encryption.

Exceptionally, in urgent cases, OFFICIAL - SENSITIVE information may be emailed unencrypted over the internet **only** where there is a strong business need to do so and only with the **prior** approval of the Authority.

13. OFFICIAL - SENSITIVE information shall only be sent when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions and subject to any explicit limitations that the authority shall require. Such limitations, including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the material.

14. OFFICIAL - SENSITIVE information may be discussed on fixed and mobile types of telephone within the UK, but not with (or within) earshot of) unauthorised persons.

15. OFFICIAL - SENSITIVE information may be faxed to UK recipients.

Use of Information Systems

16. The detailed functions that must be provided by an IT system to satisfy the minimum requirements described below cannot be described here; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.

17. As a general rule, any communication path between an unauthorised user and the data can be used to carry out an attack on the system or be used to compromise or ex-filtrate data.

18. The following describes the minimum security requirements for processing and accessing OFFICIAL - SENSITIVE information on IT systems.

a. Access: Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of “least privilege” shall be applied to System Administrators.

Users of the IT System (Administrators should not conduct „standard“ User functions using their privileged accounts.

b. Identification and Authentication (ID&A): All systems shall have the following functionality:

(1) Up-to-date lists of authorised users.

(2) Positive identification of all users at the start of each processing session.

c. Passwords: Passwords are part of most ID&A Security Measures. Passwords shall be „strong“ using an appropriate method to achieve this, for example, including numeric and “special” characters (if permitted by the system) as well as alphabetic characters.

d. Internal Access Control: All systems shall have internal Access Controls to prevent unauthorised users from accessing or modifying the data.

e. Data Transmission: Unless the Authority authorises otherwise, OFFICIAL - SENSITIVE information shall be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet, using a Foundation Grade product or equivalent as described in paragraph 12 above.

f. Security Accounting and Audit: Security relevant events fall into two categories, namely legitimate events and violations.

(1) The following events shall always be recorded:

I. All log on attempts, whether successful or failed.

II. Log off (including time out where applicable).

III. The creation, deletion or alteration of access rights and privileges.

IV. The creation, deletion or alteration of passwords.

(2) For each of the events listed above, the following information is to be recorded:

V. Type of event

VI. User ID

VII. Date & Time

VIII. Device ID

The accounting records shall have a facility to provide the System Manager with a hard copy of all or selected activity. There shall also be a facility for the records to be printed in an easily readable form. All security records are to be inaccessible to users without a need to know.

If the operating system is unable to provide this then the equipment shall be protected by physical means when not in use, i.e. locked away or the hard drive removed and locked away.

g. Integrity & Availability: The following supporting measures shall be implemented:

1. Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations)

2. Defined Business Contingency Plan

3. Data backup with local storage

4. Anti-Virus Software (Implementation, with updates, of an acceptable industry standard Anti-virus software).

5. Operating systems, applications and firmware should be supported

6. Patching of Operating Systems and Applications used shall be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk shall be documented.

h. Logon Banners: Wherever possible, a "Logon Banner" shall be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring.

a. suggested format for the text depending on national legal requirements could be: "Unauthorised access to this computer system may constitute a criminal offence".

i. Unattended Terminals: Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, or systems must activate a password protected screen saver after 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.

j. Internet Connections: Computer systems shall not be connected direct to the Internet or „untrusted" systems unless protected by a firewall (a software based personal firewall is the minimum) which is acceptable to the Authority's Principal Security Advisor.

k. Disposal: Before IT storage media (e.g. disks) are disposed of, an erasure product shall be used to overwrite the data. This is a more thorough process than deletion of files, which does not remove the data.

Laptops

19. Laptops holding any supplied or contractor generated OFFICIAL - SENSITIVE information are to be encrypted using a Foundation Grade product of equivalent as described in paragraph 12 above.

20. Unencrypted laptops not on a secure site² are to be recalled and only used or stored in an appropriately secure location until further notice or until approved full encryption is installed. Where the encryption policy cannot be met, a Risk Balance Case that fully explains why the policy cannot be complied with, and the mitigation plan, which should explain any limitations on the use of the system, is to be submitted to the Authority for consideration. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites. For the avoidance of doubt, the term "drives" includes all removable, recordable media (e.g. memory sticks, compact flash, recordable optical media (e.g. CDs and DVDs), floppy discs and external hard drives.

21. Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.

22. Portable CIS devices are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven, the CIS is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

² *Secure Sites are defined as either Government premises or a secured office on the contractor premises*

Loss and Incident Reporting

23. The contractor shall immediately report any loss or otherwise compromise of OFFICIAL - SENSITIVE information to the Authority. Any security incident involving OFFICIAL - SENSITIVE information shall be immediately reported to the Authority.

Sub-Contracts

24. The use of any sub-contractors must be stated in the Data Protection Impact Assessment (DPIA). If during the course of the contract it is decided to sub-contract work this must be reflected in an updated DPIA and this be approved by the Data Protection Officer of the CMA.

If the Sub-contract is approved, the Authority shall provide the Contractor with the security conditions that shall be incorporated within the Sub-contract document.

Publicity Material

25. Contractors wishing to release any publicity material or display hardware that arises from this contract shall seek the prior approval of the Authority. Publicity material includes open publication in the contractor's publicity literature or website or through the media; displays at exhibitions in any country; lectures or symposia; scientific or technical papers, or any other occasion where members of the general public may have access to the information even if organised or sponsored by the Authority or any other government department.

Destruction

26. As soon as no longer required, OFFICIAL - SENSITIVE information/material shall be destroyed in such a way as to make reconstitution unlikely, for example, by burning, shredding or tearing into small pieces. Advice shall be sought from the Authority when information/material cannot be destroyed or, unless already authorised by the Authority, when its retention is considered by the Contractor to be necessary or desirable. Unwanted OFFICIAL - SENSITIVE information/material which cannot be destroyed in such a way shall be returned to the Authority.

Interpretation/Guidance

27. Advice regarding the interpretation of the above requirements should be sought from the Authority.

Audit

28. Where considered necessary by the Authority, the Contractor shall provide evidence of compliance with this Security Condition and/or permit the inspection of the Contractor's processes and facilities by representatives of the Authority to ensure compliance with these requirements.

SECURITY ASPECTS LETTER

1. The above work arises from a United Kingdom government contract and will involve your company holding UK classified material. It shall be a condition of the Contract that this material must be protected. The standard of protection required has been notified to you separately and varies with the level of classification. Material passed to you will bear the classification appropriate to it. However to assist you in allocating any necessary classification to material which your company may produce during the course of the Contract and thus enable you to provide the appropriate degree of protection to it, this letter formally advises you of the correct classification to apply to the various aspects of the Contract.
2. The aspects of the Contract which require to be classified are:

ASPECTS	CLASSIFICATION
Commercially sensitive information	Official sensitive
Internal communications within the CMA	Official / Official sensitive

External communications within the CMA and other stakeholders	Official / Official sensitive
Personal data	Official sensitive

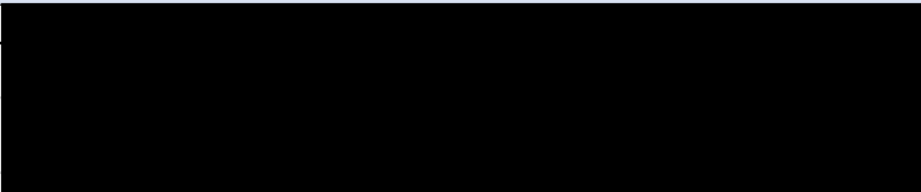
3. If the Contract contains a Condition of Clause referring to “Secret Matter” this Secret matter is defined as the Aspects listed above.

4. You are requested to acknowledge receipt of this letter and to confirm that the level of classification associated with the various aspects listed above have been brought to the attention of the person directly responsible for the security of this Contract, that they are fully understood, and that the required security controls in the contract security conditions can and shall be taken to safeguard the material concerned.

5. If you have any difficulty in interpreting the meaning of the above aspects or in safeguarding the materials, please contact Gus Cottell, Head of Security and Information Assurance, immediately on the following:

gus.cottell@cma.gsi.gov.uk or by telephone: 020 3738 6996

Minimum Pass Mark:	Completion
Fail	Information supplied is missing or incomplete
Pass	Information supplied is complete

Your Response	
Name	
Signature	
Job Title	
on behalf of	
Company Name	

14. Supplementary Terms and Conditions

Supplementary Terms and Conditions of Contract
<p>1. Authorised Representative</p> <p>1.1. The below person (including any successor in office from time to time of such person) is authorised to act as the CMA's Representative on all matters concerning this Contract:</p> <p>1.2. The below person (including any successors in office from time to time of such person) is authorised to act as the Contractor's Representative on all matters concerning this Contract:</p> <p>1.3. Each of the CMA and the Contractor may from time to time by notice in writing to the other party appoint another person to act as its authorised representative. Both parties shall use their reasonable endeavours to ensure that any such substitutions and or additions do not have any adverse impact on the Services.</p> <p>2. Indemnities and Insurance</p> <p>2.1. The Contractor shall hold harmless and indemnify the CMA on demand from and against all claims, demands, proceedings, actions, damages, costs (including legal costs), expenses and any other liabilities arising from claims made by the CMA's staff or agents, or by third parties, in respect of any death or personal injury, or loss or destruction of or</p>

damage to property, or any other loss, destruction or damage, including but not limited to financial losses which are caused, whether directly or indirectly, by the breach of contract or breach of duty (whether in negligence, tort, statute or otherwise) of the Contractor, its employees, agents or sub-contractors.

2.2. The Contractor shall be liable to the CMA for any loss, damage, destruction, injury or expense, whether direct or indirect, (and including but not limited to loss or destruction of or damage to the CMA's property, which includes data) arising from the Contractor's breach of contract or duty (whether arising in negligence, tort, statute or otherwise).

2.3. The Contractor shall effect with a reputable insurance company a policy or policies of insurance providing an adequate level of cover in respect of all risks which may be incurred by the Contractor in respect of the indemnities provided under the Contract, which in any event shall not be less than £5,000,000, and shall at the request of the CMA produce the relevant policy or policies together with receipt or other evidence of payment of the latest premium due there under.

2.4. Nothing in these Conditions or in any part of the Contract shall impose any liability on any member of the staff of the CMA or its representatives in their personal capacity.

2.5. The Contractor shall indemnify the CMA against all proceedings, actions, claims, demands, costs (including legal costs), charges, expenses and any other liabilities arising from or incurred by reason of any infringement or alleged infringement of any third party's Intellectual Property Rights used by or on behalf of the Contractor for the purpose of the Contract, providing that any such infringement or alleged infringement is not knowingly caused by, or contributed to, by any act of the CMA.

2.6. The CMA shall indemnify the Contractor against all proceedings, actions, claims, demands, costs (including legal costs), charges, expenses and any other liabilities arising from or incurred by reason of any infringement or alleged infringement of any third party's Intellectual Property Rights used at the request of the CMA by the Contractor in the course of providing the Services, providing that any such infringement or alleged infringement is not knowingly caused by, or contributed to by, any act of the Contractor.

2.7. Except in relation to death or personal injury as referred to in Condition 2.1 and subject to Conditions 2.5 and 2.6 the amount of liability under this Condition shall be limited to a sum of twice the contract value, or such other sum as may be agreed in writing between the CMA and the Contractor.

2.8. The CMA shall not be liable under to pay any sum which:

2.8.1. was claimable under insurance held by the Contractor, and the Contractor has failed to make a claim on its insurance, or has failed to make a claim in accordance with the procedural requirements of the insurance policy;

2.8.2. when added to any sums paid or due to the Contractor under the Contract exceeds the total sum that would have been payable to the Contractor if the Contract had not been terminated prior to the expiry of the Contract Duration; or

2.8.3. is a claim by the Contractor for loss of profit or any indirect or consequential loss, due to early termination of the Contract.

3. Conflicts of Interest

3.1. The Contractor shall disclose to the CMA's Representative as soon as is reasonably practical after becoming aware of any actual or potential conflict of interest relating to

provision of the Services by the Contractor or any event or matter (including without limitation its reputation and standing) of which it is aware or anticipates may justify the CMA taking action to protect its interests.

4. Survival of the Contract

4.1. Insofar as any of the rights and obligations of the parties in this Contract shall or may be exercised after expiry or termination of the Contract, the provisions of the Contract conferring such rights and powers shall survive and remain in full force and effect notwithstanding such termination or expiry or any other contract with the CMA.

5. Non-Solicitation

5.1. For the duration of this Contract and for a period of six months thereafter, the Contractor shall not directly or indirectly employ, engage or enter into any contract for works or services with any employee of the CMA with whom the Contractor has had contact during this Contract without the prior written consent of the CMA.

5.2. The Contractor acknowledges that breach of Condition 5.1 shall give rise to considerable cost being incurred by the CMA. In the event of any such breach (and for the avoidance of doubt and without limitation), the Contractor agrees to make the following payments to the CMA:

6. the full recruitment costs associated with the recruitment of a replacement for the CMA employee including but not limited to advertising, agency fees and reasonable internal management time;

7. any additional costs incurred by the CMA in the employment of temporary staff to provide cover in whole or in part for the said employee during any recruitment period; and

8. where in the reasonable opinion of the CMA the employee has received special training funded by the CMA, the Contractor shall pay the reasonable costs associated with providing additional training to any new employee.

8.1. If the CMA gives its consent to the employment of any of its employees by the Contractor such consent shall not vary or amend the duties of confidentiality owed by the said employee to the CMA or the Contractor obligations under this Contract. The CMA may at its reasonable discretion make such consent conditional on the receipt by the CMA of the payments described in Condition 5.2 above.

9. Working Time Directive

9.1. The Contractor shall ensure that the Working Time Directive Employment Regulations shall be applied in the proper manner to all personnel supplied via this Contract.

9.2. The Contractor shall ensure that commensurate with good employment practices and policies observed by the CMA, that all employment legislation is applied appropriately to all workers employed in providing the Services.

10. Observance of Statutory Requirements

10.1. The Contractor insofar as it is legally liable shall comply with all statutory requirements to be observed and performed in connection with the Contract and shall indemnify the CMA against all actions, claims, demands, proceedings, damages, costs, charges and expenses whatsoever in respect of any breach of statutory obligations.

11. Equal Opportunities and Harassment

11.1. The Contractor shall adopt a policy to comply with the requirements of the Race Relations Act 1976, the Race Relations (Amendment) Act 2000, the Employment Equality (Religion or Belief) Regulations 2003, the Sex Discrimination Act 1975 as amended,

Equal Pay Act 1970, Employment Equality (Sexual Orientation) Regulations 2003, Sex Discrimination (Gender Reassignment) Regulations 1999, and the Disability Discrimination Act 1995 and the Disability Discrimination Act 2005, and accordingly, shall not treat one individual or group of people less favourably than others because of colour, race, nationality, ethnic origin, religion, gender, sexual orientation or disability and, further, shall seek to promote equality among its workers and generally. The Contractor shall note the CMA's current and future obligations under these Acts and under the Data Protection Act 2018, Freedom of Information Act 2000, Human Rights Act 1998, and any codes of practice and best practice guidance issued by the Government and the appropriate enforcement agencies.

11.2. The Contractor shall comply with the above legislation in so far as it places obligations upon the Contractor in the performance of its obligations under this Contract. The Contractor shall facilitate the CMA's compliance with the CMA's obligations under these provisions and comply with any request from the CMA for that purpose.

11.3. In the event of any finding of unlawful racial, disability or sexual discrimination being made against the Contractor by any court or industrial tribunal, or of an adverse finding in any formal investigation by the Equality and Human Rights Commission the Contractor shall take appropriate steps to prevent repetition of the unlawful discrimination and shall on request provide the CMA with details of any steps taken.

11.4. The Contractor shall set out its policies on race relations, sex discrimination and disability discrimination:

12. in instructions to those concerned with recruitment, training and promotion;

13. in documents available to its personnel, recognised trade unions or other representative groups of its personnel; and

14. in recruitment advertisements and other literature.

14.1. The Contractor shall, on request provide the CMA with copies of its policies, examples of the instructions and other documents, recruitment advertisements and other literature.

14.2. The Contractor shall provide such information as the CMA may reasonably request for the purpose of assessing the Contractor's compliance with this Condition 7.

14.3. The Contractor shall take all reasonable steps to ensure that Contractor's personnel engaged in the performance of the Contract do not act towards either CMA staff or members of the public in a manner that could amount to harassment on any of the grounds mentioned in 7.1. In the event of any finding of unlawful discrimination being made against the Contractor by any court or tribunal, or of any adverse finding in any formal investigation, the Contractor shall take appropriate steps to prevent repetition of the unlawful discrimination and shall, on request, provide the CMA with details of any steps taken.

15. Payment

15.1. All invoices must be sent, quoting a valid purchase order number, to: The Competition and Markets Authority, Finance Team, The Cabot, 25 Cabot Square, London E14 4QZ. Within [10] working days of receipt of your countersigned copy of this letter, we will send you a Purchase Order (PO) with unique PO number. You must be in receipt of a valid PO number before submitting an invoice.

15.2. To avoid delay in payment it is important that the invoice is compliant and that it

includes a valid PO number, PO number item number (if applicable) and the details (name and telephone number) of your customer contact (i.e. Contract Manager). Non-compliant invoices will be sent back to you, which may lead to a delay in payment. If you have a query regarding an outstanding payment please contact our Accounts Payable section either by email to Finance.Team@cma.gov.uk or by telephone 020 3738 6144/6617 between 09:00-17:00 Monday to Friday.

16. Relevant Conviction

- 16.1. The CMA may require the Contractor to ensure that any person employed in the provision of Services has undertaken a Disclosure and Barring Service check. The Contractor shall ensure that no person who discloses that he/she has a conviction that is relevant to the nature of any Services, relevant to the work of the CMA, or is of a type otherwise advised by the CMA (each such conviction a "Relevant Conviction"), or is found by the Supplier to have a Relevant Conviction (whether as a result of a police check, a Disclosure and Barring Service check or otherwise) is employed or engaged in the provision of any part of the Services.

CMA Representative

Name	
Email	
Number	
Minimum Pass Mark:	Completion
Fail	Information supplied is missing or incomplete
Pass	Information supplied is complete

Your Response

Name	
Email	
Number	

15. Confidentiality and Security Requirements

Confidentiality and Security Requirements	
<p>1. The secrecy and security aspects of the Competition & Markets Authority's work are governed by section 5 of the Official Secrets Act 1989, section 101 of the Telecommunications Act 1984, section 206 of the Water Industry Act 1991, section 74 of the Airports Act 1986, section 197 of the Broadcasting Act 1990, section 145 of the Railways Act 1993, Article 49 of the Airports (Northern Ireland) Order 1994, sections 348, 350(5) and 352 of the Financial Services and Markets Act 2000, Schedule 7 of the Postal Services Act 2000, section 105 of the Utilities Act 2000, Schedule 9 of the Transport Act 2000, section 245 of the Enterprise Act 2002, Article 63 of the Energy (Northern Ireland) Order 2003, section 393 of the Communications Act 2003 and Article 265 of The Water and Sewerage Services (Northern Ireland) Order 2006 (the Acts). Contractors shall be bound by the provisions of the Acts. Contractors should ensure that they fully understand the serious consequences that which may follow from a breach of any of these confidentiality requirements.</p> <p>2. The confidentiality provisions of the Acts constitute a set of general restrictions on the disclosure of information obtained under the Acts in respect of particular businesses except when this is necessary for the purposes of the Act or for certain other prescribed purposes. Criminal prosecution is possible where unauthorised disclosure takes place. Most of the documents handled by the CMA fall within the scope of these statutory restrictions on disclosure and as 'sensitive documents' require the protection of effective security control and of strict observance of security rules. Contractors shall be expected to follow the CMA's security rules and these shall be discussed fully with them prior to commencement of the service.</p> <p>3. Part V of the Criminal Justice Act 1993 also applies to information obtained in the course of CMA inquiries. It is a criminal offence under that legislation for members of a Contractor's staff to deal, or to encourage others to deal, in securities about which they hold inside information (i.e. unpublished price sensitive information relating to particular securities), obtained by virtue of their work for the CMA, or to disclose such information otherwise than in the proper performance of their work.</p> <p>4. Contractors shall be responsible for ensuring that all staff employed in connection with any aspect of the service do not divulge any information obtained in, or as a result of, their work for the Competition and Markets Authority, except in the course of duty. The requirement not to divulge information includes not divulging information to other members of the Contractors' staff. Contractors shall also be responsible for ensuring that members of their staff are aware of and abide by the confidentiality provisions of the Acts and sign a witnessed declaration of the form set out on the following page. This requirement shall include all support staff who may be involved in system administration or other duties which require them to be given access to any part of the Competition and Markets Authority network. A copy of each of these signed declarations shall be sent to the Contract Manager.</p>	
Minimum Pass Mark:	For Information only

16. Confidentiality Undertaking

CONFIDENTIALITY UNDERTAKING, THE COMPETITION AND MARKETS AUTHORITY			
<p>I understand that in any work for 'the CMA' which I perform I shall be in possession of information which is held in confidence and which must not be disclosed without lawful authority. I am aware that the legislation referred to below provides for criminal prosecution where unauthorised disclosure takes place, and that on conviction a person may be fined or imprisoned. I am also aware that, in law, I owe duties of confidentiality to the CMA.</p> <p>I accept that I must not communicate, orally or in writing, any information gained by me as a result of my work for the CMA to any person other than a person to whom it is my duty to communicate it without the consent of the Chief Executive of the CMA (or an authorised member of his staff). In the case of information with respect to any particular trade or business, I accept that the consent of the person carrying on that trade or business is required also. I accept that articles of any description prepared for publication or discussion in any written form or for broadcasting are covered by these conditions.</p> <p>I also acknowledge that Part V of the Criminal Justice Act 1993 applies to me and that it is a criminal offence to deal, or to procure others to deal, in securities about which I hold unpublished price sensitive information when engaged in work for or on behalf of the CMA.</p>			
Minimum Pass Mark:	Completion		
Fail	Information supplied is missing or incomplete		
Pass	Information supplied is complete		
Your response			
Name		Date	05/01/2024
Signature			
Witness		Date	05/01/2024
Your Offer ref	PROC 732-2023		
While the Contractor is working at the CMA's offices, the following people are to be contacted in case of an emergency:			
Your response			
Name			
Job title			
Name of Company	Methods Business and Digital Technology Limited		
Phone Number			

Conflicts of Interest in Relation to Contractors and Contractors' Staff
<p>Summary</p> <ol style="list-style-type: none"> Contractors and their staff must disclose any interests which might give rise to a conflict or potential conflict to the CMA before entering into a contract with the CMA. The CMA will consider whether the potential conflict causes concern and what action (if any) should be taken. It may be necessary to require the disposal of an interest in order for the CMA to be able to enter into a contract. <p>Detail</p> <ol style="list-style-type: none"> When a Contractor is approached with a view to entering into a contract or call-off with the CMA, the Contractor must disclose to the CMA any potential conflict of interest of which it is aware, or becomes aware, affecting any of the following: <ol style="list-style-type: none"> the Contractor, their spouse, or partner (other than a spouse) and dependents; all personnel of the Contractor whose involvement on a contract with the CMA is not purely mechanical or clerical; and all directors, partners and other senior personnel of a Contractor with equivalent responsibilities even though they are not involved in a contract with the CMA. If the Contractor has any doubts as to whether or not there exists an interest which may give rise to a conflict, these doubts must also be disclosed. In this annex the following terms have the meanings set out below: <ol style="list-style-type: none"> "relevant individuals" means persons within sub-paragraphs 2 (a) to (c) above, together with their spouses, partners (other than a spouse) and dependents; "the reference companies" means any company (incorporated or unincorporated), partnership, business or individual that is the subject of the reference relating to the Contract or Call-off to be awarded to the Contractor; "the relevant companies" means any company (incorporated or unincorporated), partnership, business or individual who is a competitor, customer or supplier of any reference companies. "shareholding" includes: <ol style="list-style-type: none"> shares, whether bearing a right to vote or not; stock or debentures; and options and similar rights; in each case whatever the value of the holding and whether held as trustee or beneficially, (for example under a family trust or a Personal Equity Plan). Holdings in unit trusts, investment trusts, unit linked policies or similar arrangements under which the investor has interests in a large number of enterprises would not normally give rise to a potential conflict of interest, unless any company involved in the arrangements were itself affected by the inquiry. However, if the trust or arrangement specialises in investing in a particular industry which is affected by the reference or if the investor believes that there is a real possibility of the value of the investment being affected by the outcome of the reference, the interest should be disclosed to the CMA. The requirement under paragraph 3 to disclose any potential conflict of interest includes a requirement to disclose any relationship which may give an appearance of bias on the part of the Contractor or its staff including but not limited to: <ol style="list-style-type: none"> the Contractor's present or past contractual relationship with any of the reference companies; the Contractors' present or past contractual relationship with any of the relevant companies;

- c. the Contractor's or relevant individuals' shareholding or partnership in, ownership (whether full or partial) or directorship of, or employment by:
 - (i) the reference companies;
 - (ii) the relevant companies; and
 - (iii) any enterprise the value of whose shares may be affected by the outcome of the reference (e.g. an enterprise in the same industry).
 - d. the Contractor's present or past contractual relationship with, or the Contractor's, or relevant individuals', employment by the relevant regulator (if applicable in relation to the reference);
 - e. the management of the investment of a shareholding or other interest of a person for which the Contractor, or any relevant individual, is responsible; and
 - f. a recent personal or family involvement with the reference companies or the relevant companies e.g. a substantial shareholding or other interest which has recently been disposed of.
6. Share accounts with a building society would not need to be disclosed except, for example, where they entitled the holder to a "perk" in the event of a merger. Similarly, bank accounts would not normally need to be disclosed in a reference involving the bank, though they should be disclosed where a person wishes to obtain or renegotiate a loan or overdraft.
 7. A potential conflict of interest may arise in other circumstances, such as where there is a business relationship with an enterprise affected by the reference or any other close relationship with a person whose affairs may be affected by the reference. **In case of doubt the Contractor or relevant individual should disclose the interest.**
 8. An interest as a consumer would not need to be disclosed, in normal circumstances, where the value of the goods or services obtained is small or most individuals are consumers (e.g. in the case of a market investigation into the supply of milk, salt or bread). If however the interest is that of a minority class of consumer there might be a conflict. This might be the case if, for example, an individual, his or her spouse, or child, were a coeliac and as such required gluten free products which were produced by companies involved in a merger reference.
 9. The Contractor should check and relevant individuals as defined in paragraph 4 above should be required by the Contractor to check (if they are not already confident of the facts) their own shareholdings and shareholdings held on their behalf. They should also check, information which has been provided to them, e.g. as trustees or a holder of a specialised unit trust and whether they are aware in general terms of any conflict of interest.
 10. The CMA will decide whether anything which has been disclosed as a potential conflict of interest constitutes an actual conflict in the particular circumstances. In some circumstances it may suffice for an interest which does give rise to a conflict to be disposed of in the period between public announcement of the reference and distribution of relevant papers, (subject to the approval of the CMA). In some circumstances it may be sufficient simply to inform the parties involved in the inquiry or likely to be involved of the interest (be it a shareholding or other interest).

CONFLICTS OF INTEREST STATEMENT


THE COMPETITION AND MARKETS AUTHORITY

1. We confirm that there is no conflict of interest that might give rise to a risk of challenge in the courts to the inquiry on the ground of bias (whether actual or apparent). The acceptance of the following terms and conditions shall be taken as confirmation that no such conflicts of interest exist.

2. We shall ensure that actual or even potential conflicts do not arise during the course of the inquiry. In particular:
- a) For the duration of the inquiry we shall not undertake or actively seek any work for any organisation that is directly related to the subject of the inquiry. We agree that work which is indirectly related other than that laid out in the contract should only be undertaken with the CMA's consent which shall not be unreasonably withheld.
 - b) We confirm that any individuals providing services to the inquiry, as applicable, shall not carry out any work related to the subject of the inquiry for any other client for the duration of the inquiry. However, those individuals may consult colleagues who are engaged in such work in order to obtain information from them.
 - c) We confirm that individuals providing services to the inquiry and their immediate families do not own or have a beneficial interest in the shares of the main parties to the inquiry or their suppliers unless such holdings are independently managed (e.g. by a unit trust or pension fund).
 - d) All information acquired by the individuals providing services to the inquiry shall be treated as confidential to the CMA both for the duration of the agreement and thereafter. The individuals shall not communicate it to third parties or other individuals within your firm unless it has already entered the public domain by other means. All documents supplied to us in connection with the inquiry and this agreement, copies of any part of such documents, whether in electronic or material form, and any documents prepared by us which are based on material supplied in connection with this inquiry, must be returned to the CMA at the end of the inquiry, or sooner if requested.
3. The CMA may terminate this contract at any time should it become of the opinion that an actual or potential conflict of interest on our part has arisen. We shall be entitled to remuneration on the basis set out in this letter up to the date of termination save in circumstances where we are in breach of our obligations under the terms of the contract.
4. It shall be our responsibility to ensure that no conflict of interest arises which might be said to prejudice our independence and objectivity in performing the contract. This responsibility includes all of our senior staff (e.g. directors, and partners) or our personnel whose involvement on the contract with the CMA is not purely mechanical or clerical. If we are at any time in doubt about whether any conflict of interest may exist or arise, we shall notify the CMA forthwith and comply with any directions given with a view to avoiding the conflict.
5. During the period of the contract, and for an **agreed period** after it ends, we would, **except with the prior written consent of the Contract Manager**, be debarred from working for, or having any other interest in, any of the main parties to the inquiry (which is the subject of the Contract) or any of their competitors in the relevant industry. This requirement is made to avoid conflicts of interest.
6. The acceptance of these terms and conditions shall be taken as confirming agreement on all of the above points.

**Minimum Pass
Mark:**

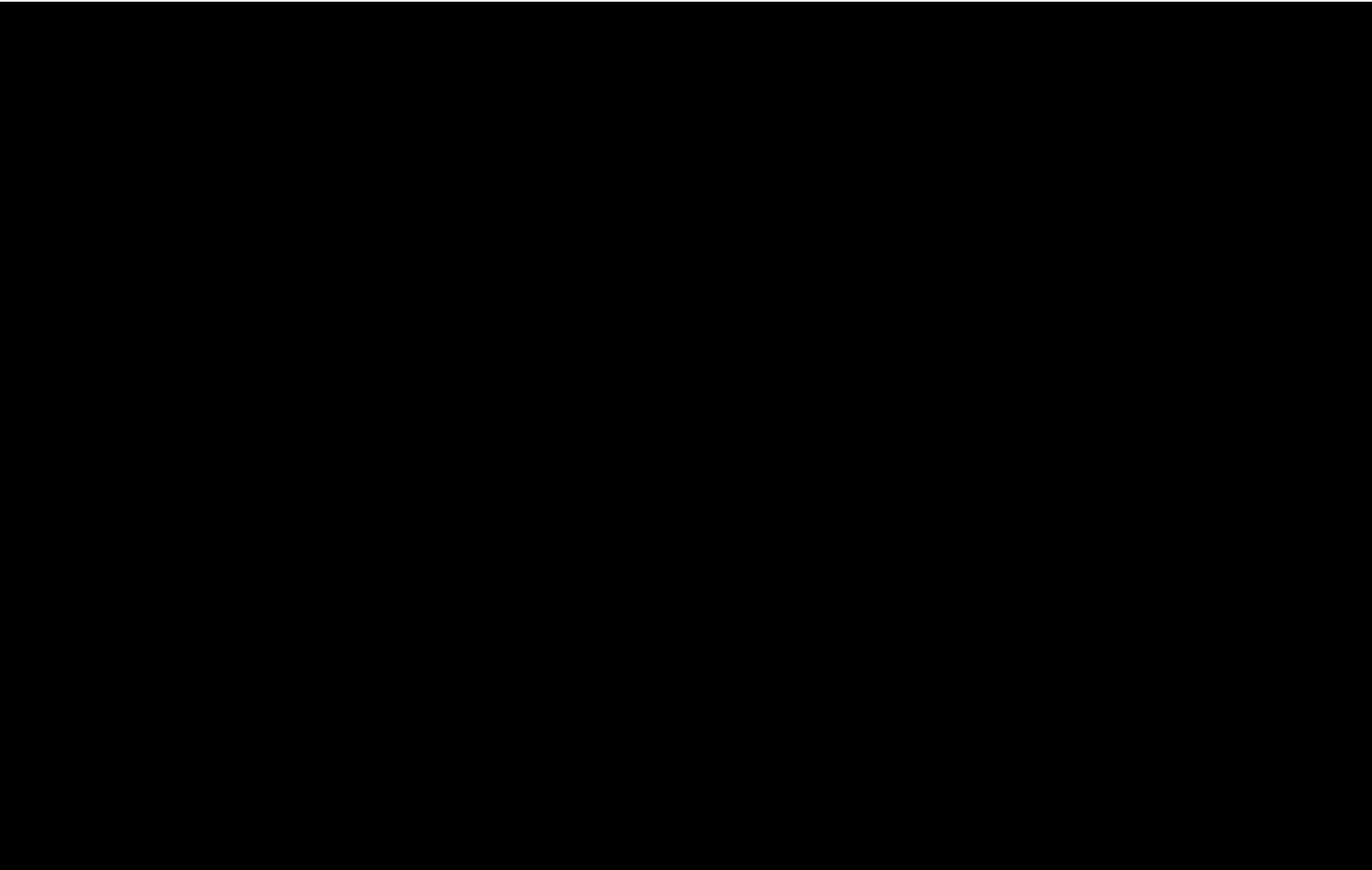
Completion

Fail	Information supplied is missing or incomplete		
Pass	Information supplied is complete		
Your Response			
Name		Date	05/01/2024
Signature			
Job Title			
on behalf of:			
Company Name	Methods Business and Digital Technology Limited		

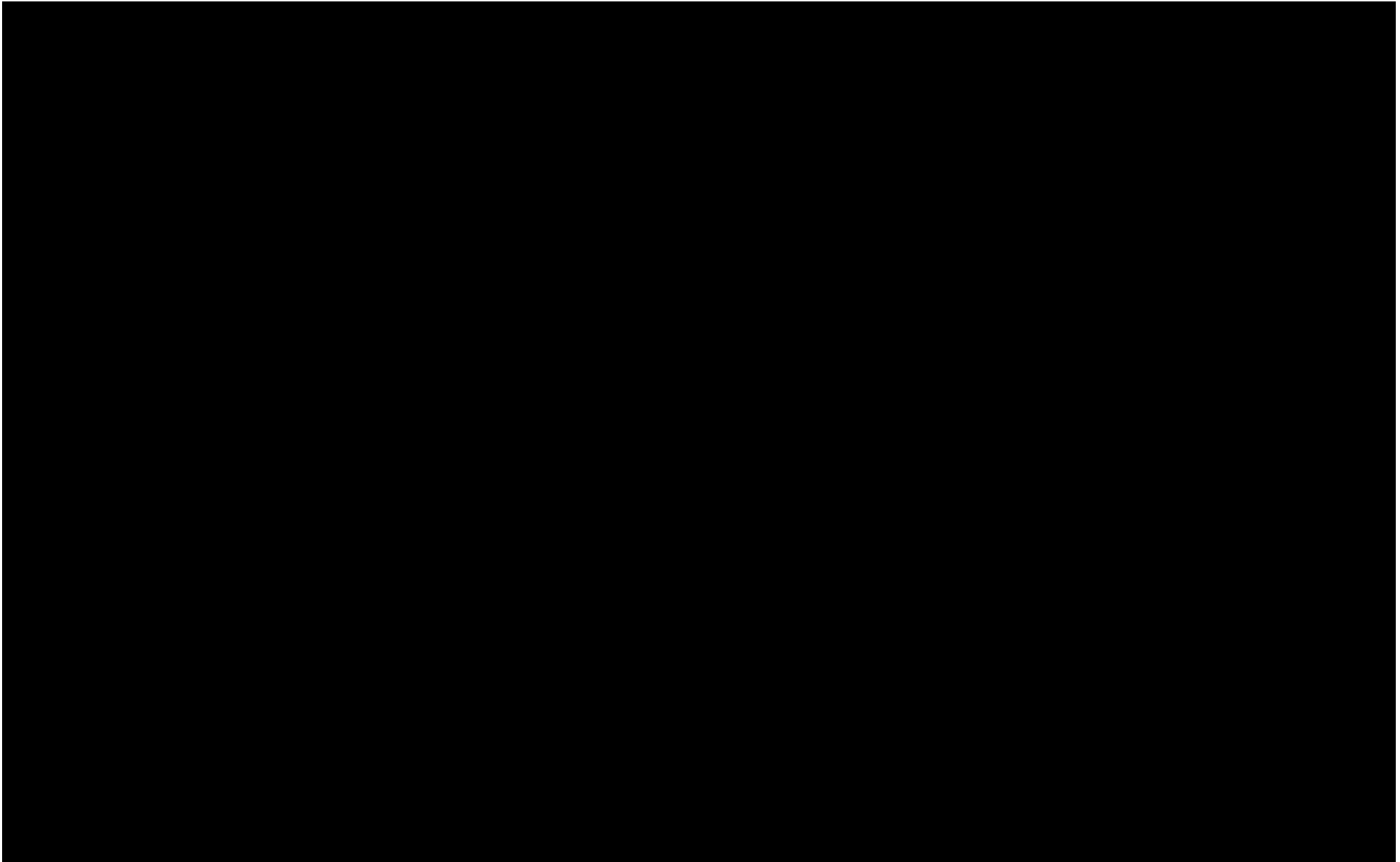
18. Data Handling Assessment

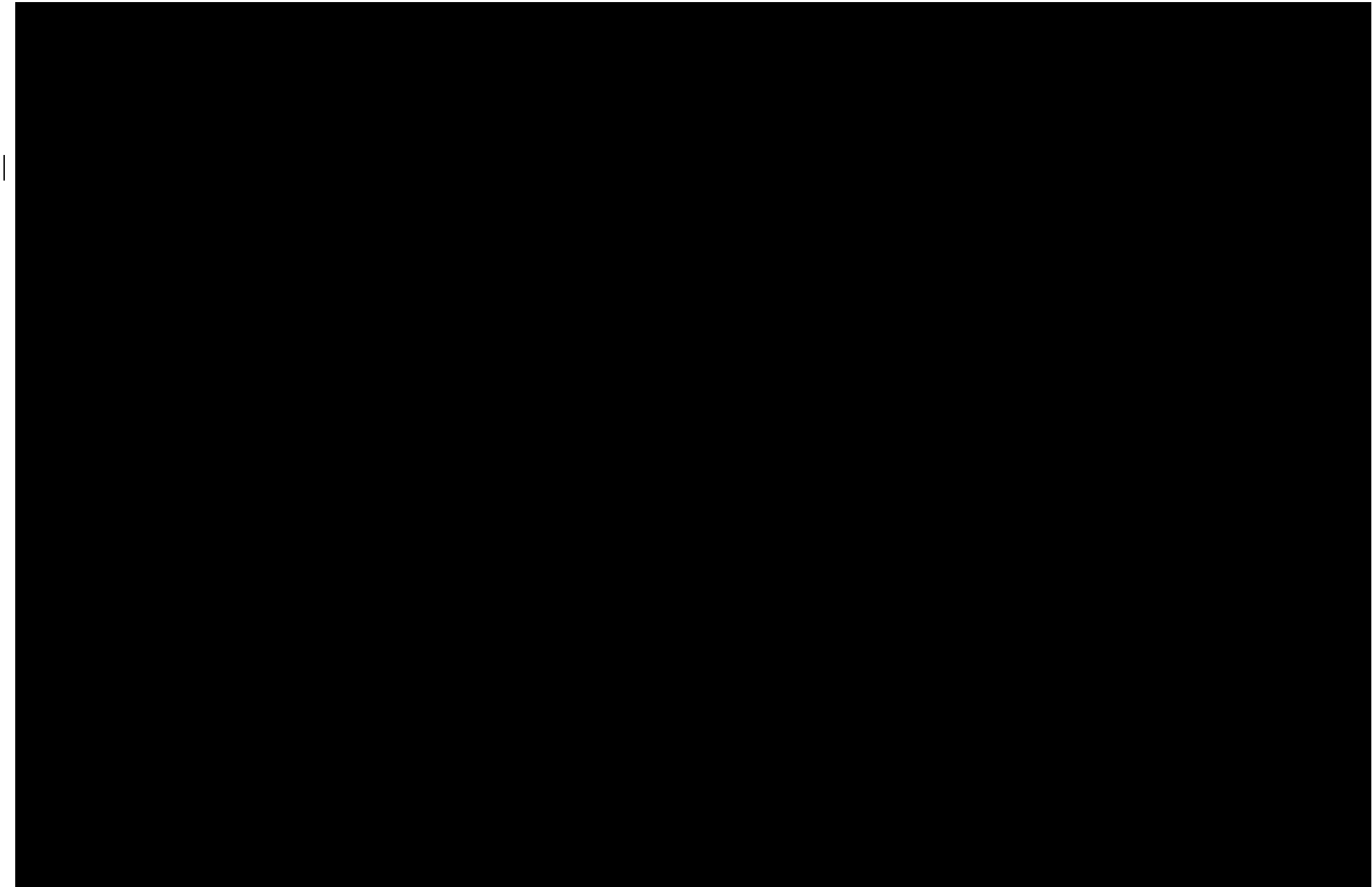
Data Handling Assessment			
Requirement:	<p>CMA requires all bidders to complete the below Data Handling Assessment as part of their offer</p> <p>Question 1: In answering this question, Tenderers should: Provide a response of 'Yes' to confirm Compliance with the CMA's requirement or 'No', to confirm non-compliance.</p> <p>Question 2: In answering this question, tenderers should: Provide a response of 'Yes' to confirm Compliance with the CMA's requirement or 'No', to confirm non-compliance. If the Tenderer confirms a response of 'Yes', the tenderer is also required to advise which country.</p> <p>Question 3: In answering this question, tenderers should: If applicable, provide a response of 'Yes' and provided a draft IDTA and we agree to conclude this with the CMA or 'No', we have not provided a draft and shall not accept IDTA or N/A if the question doesn't apply.</p> <p><i>Bidders who intend to process the CMA's data outside of the UK in performance of this contract, which cannot accept the relevant Standard Contractual Clauses (SCC) where still applicable or International Data Transfer Agreement, may fail.</i></p> <p>Question 4: In answering this question, tenderers should: Provide details of any technical and organisational measures implemented.</p> <p>Question 5: In answering this question, tenderers should: Provide a list of any documented policies and processes your company has in place.</p> <p>Question 6: In answering this question, tenderers should: Provide all geographical locations which your company will be providing all or part of the contracted services to the CMA.</p>		
	Minimum Pass Mark:	Completion	
	Fail	Information supplied is missing or incomplete	
	Pass	Information supplied is complete	
	YOUR RESPONSE		
	No.	Question/Requirement	Response
1.	Please confirm whether or not your company will process/transfer any of the Authority data in the UK.	Yes	
1.a	<i>In case of question 1 above response is "No", in which countries will your company process/transfer the Authority's data?</i>		
2.	Please confirm whether or not any of your company's sub contractors/sub processors will process/transfer any of the Authority data in the UK	Yes	
2.a	<i>In case of question 2 above response is "No", in which countries\ will your sub-contactors/processors process/transfer the Authority's data?</i>		
3	If you have advised of a country outside of the United Kingdom, you will be required to provide a draft of the Interna-	N/A	

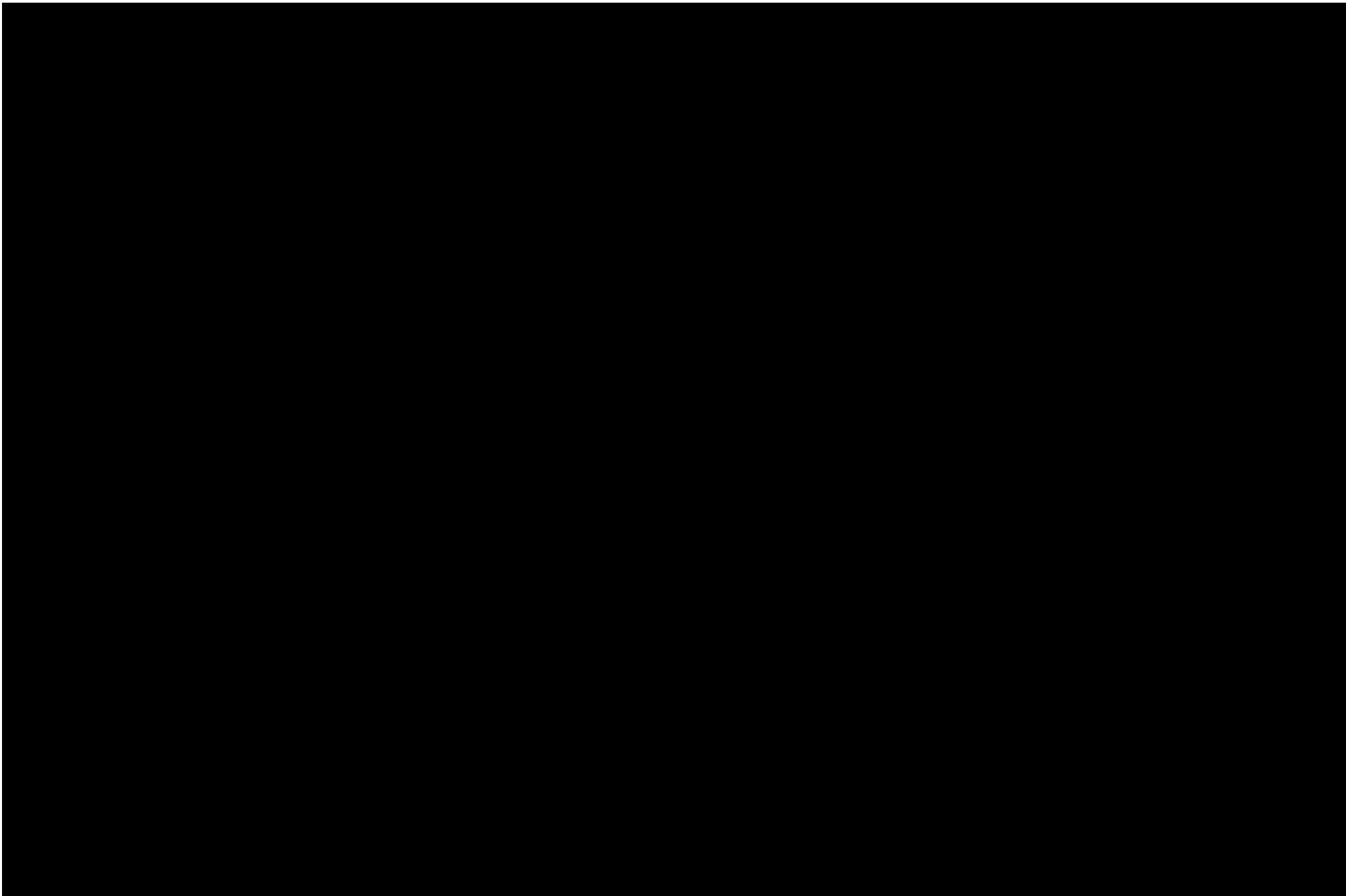
	<p>tional Data Transfer Agreement (IDTA) as issued by ICO International data transfer agreement and guidance and to conclude this with the CMA that covers all roles.</p>	
4	<p>Provide full details of any technical and organisational measures implemented to protect Personal Data in compliance with the data security requirements of the data protection legislation.</p>	<p>Methods is ICO registered and certified to ISO27001, ISO9001 and Cyber Essentials Plus.</p> <p>Methods Information Security Management Plan ensures the continuity and protection of the business processes and information assets and provide guidance on how IT systems (hardware and software) are securely configured to maximise the protection of the confidentiality, integrity and availability of data processed. This guidance enables the organisation to have mechanisms and processes to:</p> <ul style="list-style-type: none"> • Implement the concept of least privilege. • Implement a baseline configuration. • Harden host systems. • Harden operating systems. • Compliance Monitoring and alerting
5	<p>List any documented policies and processes your company has in place to support their data protection obligations e.g. Breach Management & Notification, Data Subject Rights etc.</p>	<ul style="list-style-type: none"> • Cyber Incident Response Plan • Business Continuity Plan • DPA/GDPR Policy and Processes that cover all principles and resulting actions including breach and SARs.
6	<p>Clearly specify all geographical locations from which your company will be providing all or part of the contracted services to the CMA. This includes any cloud based hosting, third party SaaS services, customer support services, third party contractors or agencies processing on behalf of the bidders and geographical location of permanent and/or temporary staff involved in providing services to the CMA.</p>	<p>Methods core systems are Microsoft O365 and Salesforce both are hosted in the UK.</p>

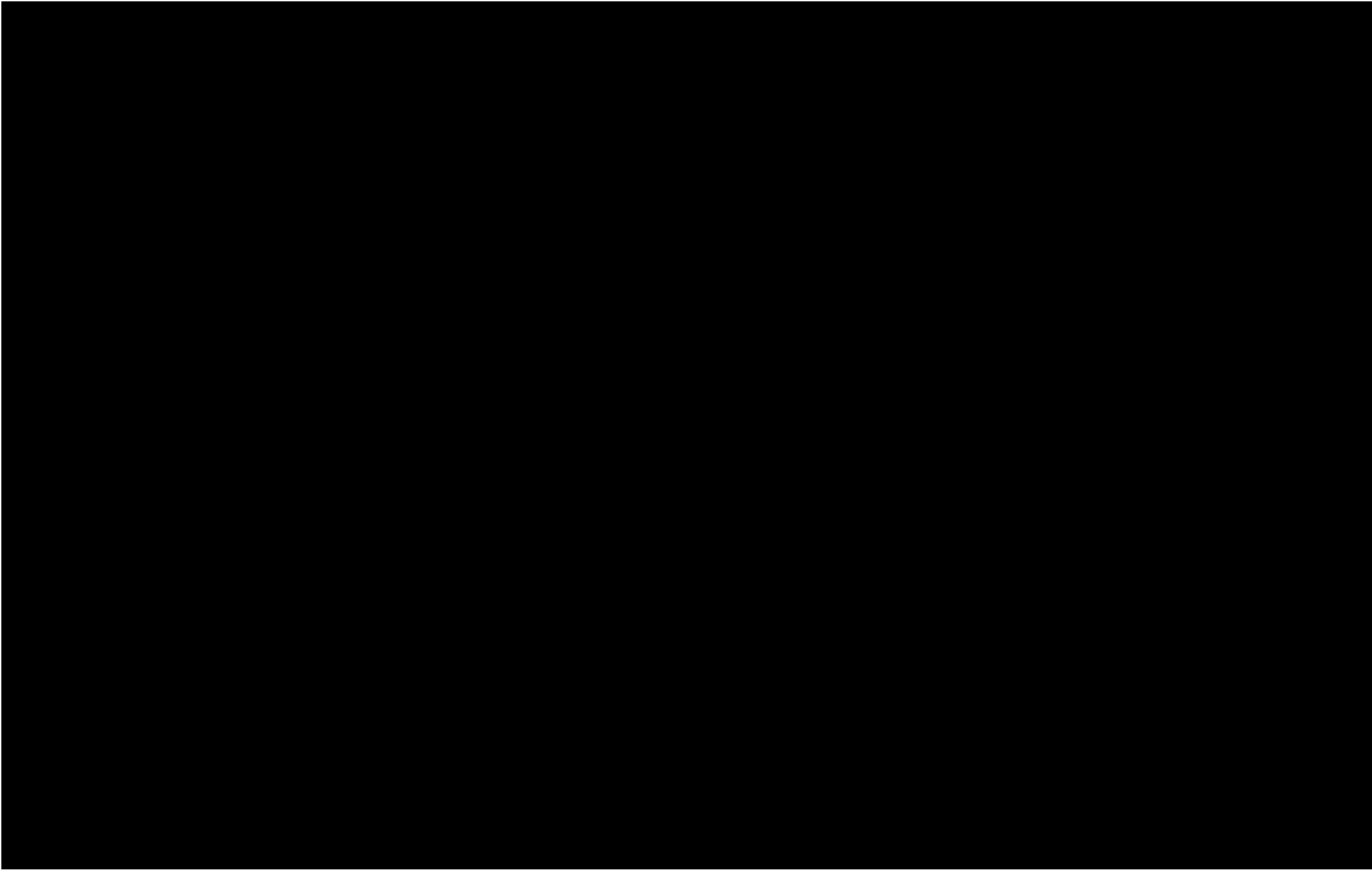


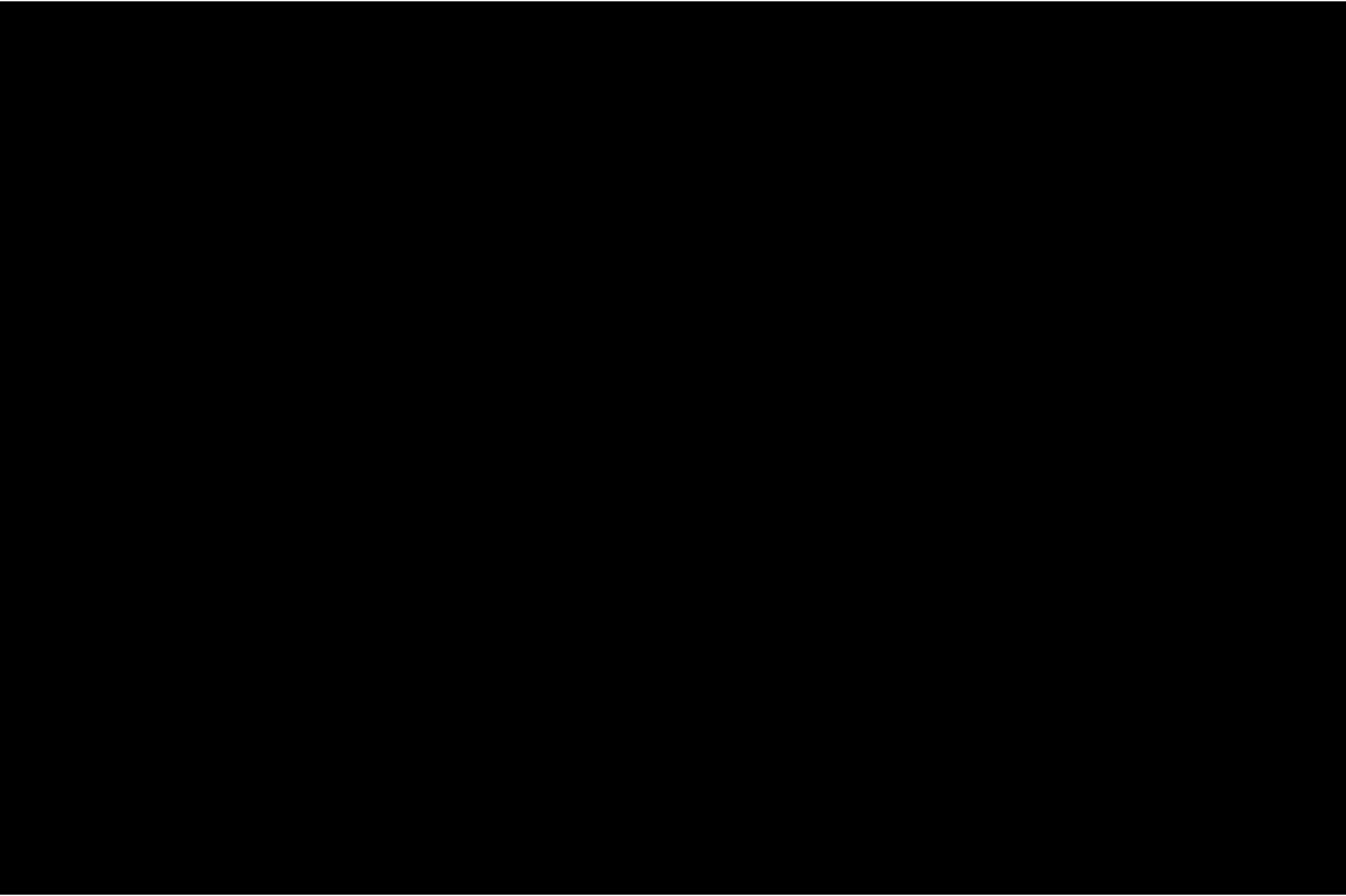
Appendix 3 - ICT Operational Services ITT clarifications

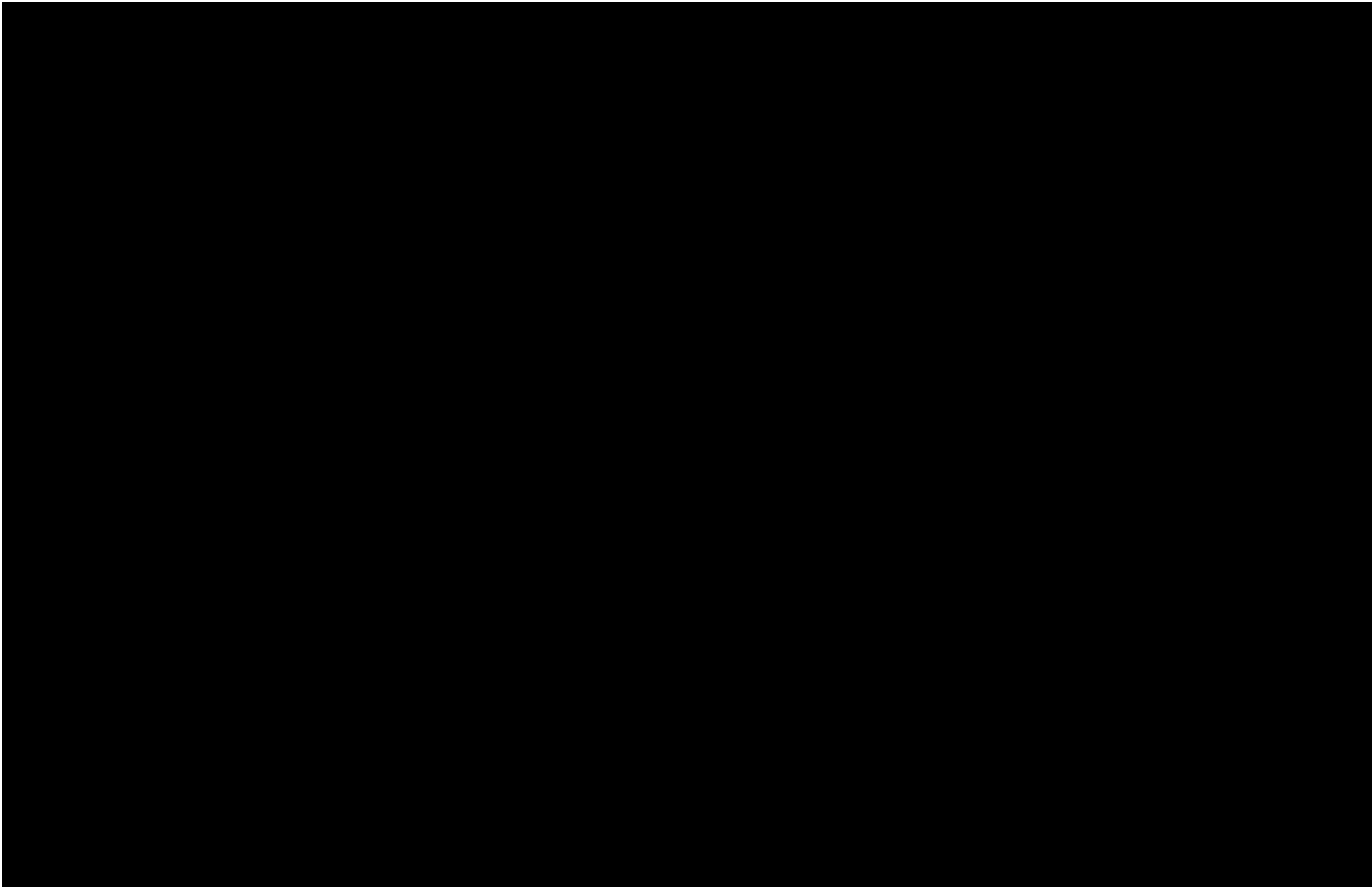












|

