



**Crown
Commercial
Service**

CALL-OFF CONTRACT

Cyber Security Services 2 RM3764ii

PART A Order Form , Specific Terms and
PART B Schedules
PART C RM3764ii Standard (non-variable)Terms
(held online)

Buyer Ref:	CCIS17B82
Date sent to supplier:	01/03/2018
Purchase Order Number:	

This agreement is between:

the “Buyer”

Independent Inquiry into Child Sexual Abuse (IICSA)
PO Box 72289 London SW1P 9LF

the “Supplier”

Aristi Ltd

Supplier No:

Innovation Centre, Longbridge Yechnology Park, 1 Devon Way, Longbridge, Birmingham. B31 2TS
(registered office address)

Together the “Parties”

Service delivery contact details:

Buyer:	Name:	REDACT
	Title:	
	Email:	REDACT
	Telephone:	REDACT
Supplier:	Name:	REDACT
	Title:	
	Email:	REDACT
	Telephone:	REDACT

PART A – ORDER FORM

This Order Form is issued in accordance with the Framework Agreement Cyber Security Services 2-RM3764ii and the Buyers mini competition tender.

The Contract is made up of:

- **Part A** – The Order Form (an overview of the services to be provided throughout the lifetime of the agreement) and the Specific Terms (which are specific to this Contract)
- **Part B** – Schedules (the Buyers requirements, the winning suppliers bid and the agreed work to be carried out) and;
- **Part C** – Standard RM3764ii Call-Off Terms and Conditions (which are non-variable)

The Supplier agrees to supply cyber security services specified below on and subject to the terms of this Contract.

The Buyer will complete the Order Form prior to the Contract award.

Call-Off Contract term:

1. **Commencement Date:** [21/03/2018]
2. **Length of Contract:** Two (2) years with the provision of a further 12 months

Contract Charges and payment

3. **The method of payment for the Contract Charges** (GPC or BACS): [BACS]
4. **Invoice details**
 - 4.1. Where and how to send invoices [Payment can only be made once the agreed tasks are completed]
 - 4.2. Who to send invoices to: [Invoices should be sent to:
Finance, The IICSA, PO Box 272289, London. SW1P 9LF
Email: Finance@iicsa.org.uk]
 - 4.3. Invoice information required: *e.g. PO, Project* [Payment can only be made once the agreed tasks are completed]
5. **Invoice Frequency** [Payment can only be made once the agreed tasks are completed]
6. **Contract Charges** [As per the below]

REDACT

Buyer contractual requirements:

7. **Services required: *** For the supply of Penetration Testing part of project ref: CCIS17B82.
Please note extent of the services exclude hardware devices and/or software products.
8. **Delivery Location(s)/Premises:** Remote although where there is a need to attend site the Supplier can choose from London, Cardiff or Sheffield.
9. **Relevant convictions:** N/A
10. **Staff Vetting and Security Clearance:** SC Clearance
11. **Local health and safety procedures:** N/A
12. **Non-Disclosure requirements:** N/A
13. **Exit Planning:** N/A
14. **Security Requirements:** All staff are required to have SC Clearance
(including details of Security Policy and any additional Buyer security requirements) **
15. **Protection of Buyer Data:** The Authority will own all IPR of all documentation provided to the Supplier.
Any reports written following testing will remain the property of the Supplier. However any further documentation produced by the Authority as a result of the testing belongs to the Authority, even if it includes portions of the test report content
16. **Standards:** The Suopplier must hold NCSC Check Accreditation
17. **Business Continuity and Disaster Recovery:** N/A
18. **Insurance:** As per Clause 16 of the framework agreement RM3764ii

*Liability Insurance – minimum level of cover
£5,000,000*

*Professional Indemnity – minimum level of cover
£2,000,000*

Additional and/or alternative clauses:

This section allows the Buyer to add supplemental requirements and additional terms to the Contract. These must be completed before the requirements are published.

19. **Supplemental requirements in addition to the Call-Off Terms** [Click here to enter text.](#)

20. **Buyer Specific Amendments to the Call-Off Terms**

The table below lists the editable terms from the RM3764ii Standard Call-Off Terms.

The number of days, value or other elements of these terms may be increased to suit the Buyer's needs. They may not be decreased. When amending these terms, the Buyer must state whether it has been increased or not.

Clause	Heading	Minimum Contract term (cannot be reduced)
4	Warranties and Representations	Will remain 90 Working days from the date the Buyer accepts the release of work.
18	Supplier Assistance at Retendering	Will remain 10 Working days
24	Force Majeure	Will remain 15 consecutive Calendar Days
19	Changes co Contract	Will remain 5 Working Days
37	Dispute Resolution	Will remain that active efforts will be made to resolve within 10 working days
38	Liability	Will remain <ul style="list-style-type: none"> • direct loss or damage to property - £1,000,000 in each Contract Year in which the default occurred or is occurring • £500,000 or a sum equal to 200% depending on the liability damage/loss or impact
39	Termination Events Material Breach	Will remain 15 consecutive Calendar Days

Further information:

** Security Requirements Note:

If the Buyer requires work to be carried out at the OFFICIAL-Sensitive status or above, the Parties agree to complete a Security Aspect Letter to accompany the contract award.

The Buyer may choose to issue a specific Security Aspects Letter to determine the security of the work undertaken.

What is a security aspects letter?

Find out more: <https://www.gov.uk/guidance/defence-equipment-and-support-principal-security-advisor#frequently-asked-questions>

Winning Supplier's information:

21. Suppliers commercially sensitive information

Winning supplier to confirm any commercially sensitive information from their bid.

22. Key Sub-Contractors

Winning supplier to confirm details of any sub-contractors are being used. (name and role)

23. Contract Charges

[REDACT]

Acknowledgment:

- By signing and returning this Call-Off Contract the Supplier agrees to enter into agreement to supply Cyber Security Services to the Buyer as described in Cyber Security Services 2 RM3764ii.
- The Parties acknowledge and agree that they have read the Call-Off Contract and RM3764ii Standard Call-Off Terms and by signing below, agree to be bound by this Contract.
- The Parties acknowledge and agree that this Contract shall be formed when the Buyer acknowledges the receipt of the signed copy from the Supplier within two (2) Working Days. Ref: RM3764ii Call-Off Procedure)
- The Contract outlines the deliverables and expectations of the Parties. Order Form outlines any terms and conditions amended within the Call-Off Contract. The terms and conditions of the Call-Off Order Form will supersede those of RM3764ii Standard Terms.

SIGNED:

	Supplier: ARISTI LTD.	Buyer:
Name:	REDACT	REDACT
Title:	MR	MR
Signature:	REDACT	REDACT

PART B – THE SCHEDULES

Remove all guidance when complete

SCHEDULE 1 – SERVICES NEEDED

THE REQUIREMENT

The Authority's IT estate is cloud hosted and the following is a high level list of the current technologies consumed by the Authority:

- REDACT

This requirement seeks a Supplier with a broad range of skills in the technologies above, as well as strong capabilities in cloud technology, in order to fulfil the Authority's penetration testing needs.

The Authority also has a prominent social media presence and therefore requires a Supplier that can provide threat assessment based on public activity in forums such as Twitter, Facebook and other social media applications.

The Supplier may also be required to assist the Authority as and when required in testing any new system or change to existing system.

The Supplier will be responsible for conducting penetration testing for the Authority as and when the Authority deems necessary over the course of this contract. It is anticipated that testing will be required on average four (4) times a year, however this is not a guaranteed volume of work. The demand may vary on the development and implementation of new systems or changes to the existing system.

Scope of testing

When a penetration test is required, the Supplier will be responsible for working in direct collaboration with Authority's security experts to ensure tests are thorough and all potential risks are identified.

The Supplier must acknowledge receipt of the test within 48hrs and have sufficient resources in place to complete the testing within 4 weeks of initial contact.

Each activity shall be defined in collaboration prior to testing and will should include the following steps:

- Initial engagement;
- Definition of scope;
- Validation of scope;
- Testing activities;
- Daily wash-ups;
- Initial highlight report;
- Full report;
- Guidance with remediation;
- Retest of remediated vulnerabilities;
- Sign-off.

Prior to the commencement of testing, the Supplier must provide a detailed scope of testing based on meeting discussions and written descriptions of the system provided by the Authority or its third party providers. This should be agreed upon with the Authority prior to the commencement of the test.

Testing Expectations and Deliverables

The Supplier must provide independent security assessment of the Authority's applications and systems using industry standard techniques to identify potential vulnerabilities.

During the testing stage the Supplier must facilitate in a daily wash-up meeting via google hangout and provide an initial report with 24hrs.

The Authority operates within the Google G-Suite environment using Chrome OS devices, therefore is not able to work with some Microsoft proprietary formats.

All information shall be uploaded to the Authority's Google supplier domain for sharing with the Authority, where required. Egress switch may also be used to transfer information. No Authority information shall be stored on the suppliers systems.

The Supplier will be expected to provide assurance details, upon request, of any hardware and software used to perform the testing.

The Supplier will be required to verify and provide proof of deletion of any data collected during the test at the closure of each activity. This will be agreed with the Authority when defining the test scope.

Reporting

The Supplier will be required to provide a comprehensive written report, as defined within the NCSC CHECK scheme standard, listing all vulnerabilities identified during the test.

Following the assessment the Supplier must provide to the Authority, within 2 weeks (10 working days,) a written statement, that can be viewed in Google chrome, listing the following:

All identified vulnerabilities and their associated likelihood

Associated impact, and

Recommendations for remediation.

The Authority reserve the right to seek clarification, at any time, of any report reviewed as and when required.

Location

Given the Authority's cloud based platform, it is anticipated 80% of testing will be done remotely. Where there is a need to attend site, the Supplier is able to choose their preferred site of attendance from London, Cardiff or Sheffield.

KEY MILESTONES

Not applicable.

AUTHORITY'S RESPONSIBILITIES

The Authority will be responsible for providing all relevant and appropriate documentation pertaining to the system to be tested upon test identification.

Where applicable, the Authority shall facilitate meetings, whether physical or virtual location, and ensure all relevant parties are invited. The Authority will further circulate all relevant documentation to attendees' prior and following discussion, as appropriate.

The Authority will be responsible for reviewing all test reports provided by the Supplier.

REPORTING

Various reports are needed throughout this contract, please refer to section 6.

VOLUMES

It is anticipated the Authority will require Penetration Testing services on average four (4) times a year. The demand may vary on the development and implementation of new systems or changes to the existing system.

CONTINUOUS IMPROVEMENT

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

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

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

SUSTAINABILITY

Not applicable.

QUALITY

The Supplier must hold a National Cyber Security Centre (NCSC) CHECK accreditation and provide the link to the NCSC website to support this.

PRICE

Day rates will be used as the charging mechanism for this contract and as such Potential Providers are required to provide fixed day rates per job role as identified in Appendix E – Pricing Schedule.

It is anticipated that 20% of testing will be conducted at one (1) of the four (4) locations listed in section 6.19, depending on the Supplier's preference. Potential Providers are therefore required to outline firm Travel and Subsistence (T&S) costs in association with the travel to the Provider's preferred location for these tests.

Based on the testing requirements on site, the Authority anticipates that T&S costs will only apply to the "CHECK Team Leader – Web Apps" job role.

Any travel required in addition to/or outside of the locations specified in this document will only be paid if agreed in advance and in line with the Authority's Internal travel policy limits.

Prices are to be fully outlined in Appendix E – Pricing Schedule and should be supported by an official letter-headed quotation.

Prices are to be submitted via the e-Sourcing Suite excluding VAT.

STAFF AND CUSTOMER SERVICE

The Authority requires the Supplier to provide a sufficient level of resource throughout the duration of the Penetration Testing Contract in order to consistently deliver a quality service to all Parties.

Supplier's staff assigned to this Contract shall have the relevant qualifications and experience to deliver the Contract.

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

SERVICE LEVELS AND PERFORMANCE

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

KPI/SLA	Service Area	KPI/SLA description	Target
1	Delivery timescales	Acknowledgment and receipt of initial test within 48hrs.	100%
2	Delivery timescales	Daily wash-up meeting via google hangout and provide an initial report with 24hrs.	100%
3	Delivery timescales	Written statement with 2 weeks (10 working days)	100%
4	Delivery timescales	Facilitate testing within 4 weeks of initial contact.	100%

In the event of a missed target against the SLA's/KPI's outlined above, the Authority will work with the Supplier to address these failings and remedy them as appropriate.

In the event of a missed target, the Authority reserves the right to withhold payment until a point at which the resolution to this has been resolved.

SECURITY REQUIREMENTS

All staff working for the Supplier is required to hold SC security clearance as a minimum.

INTELLECTUAL PROPERTY RIGHTS (IPR)

The Authority will own all IPR of all documentation provided to the Supplier.

Any reports written following testing will remain the property of the Supplier. However any further documentation produced by the Authority as a result of the testing belongs to the Authority, even if it includes portions of the test report content.

PAYMENT

The Supplier will enter an agreement with the Authority based on the specific task required on a per project basis.

Payment can only be made once the agreed tasks are completed, the Supplier will be able to invoice the Authority and payment will ensue in due course.

Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

Invoices should be sent to:

Finance
The IICSA
PO Box 72289
London
SW1P 9LF

And by e-mail to: finance@iicsa.org.uk

ADDITIONAL INFORMATION

The Authority wish to make it known that this is not a requirement for a specific set of tests. No specific tests are defined at this stage.

Testing will be required on a "call-off" basis. Volumes of work have been provided for indicative purposes only and the total volume of work conducted under this contract cannot be guaranteed.

Subcontracting and Partnering will be permitted under the terms and conditions of this requirement.

LOCATION

The location of the Services will be carried remotely although the Authority may require on-site testing as and when required.

SCHEDULE 2 - HIGH LEVEL DELIVERY PLAN

Insert the Suppliers high-level delivery plan. Take this from their bid from the mini competition tender.

There is no high level delivery plan as yet as there is no confirmed scope, it is all based on a day rate.

SCHEDULE 3 - BUYER RESPONSIBILITIES

Winning supplier to add any responsibilities of the Buyer here. Include anything that the Supplier needs the Buyer to do, to enable them to do their job.

These will be decided as each test's scope is defined.

SCHEDULE 4 – NON-DISCLOSURE AGREEMENT

Optional to include at the Buyers discretion N/A

SCHEDULE 4 – STATEMENT OF WORK (SoW)

This schedule outlines the work to be carried out within each delivery stage.

A new SoW needs to be created for each delivery package.

This is the order to the Supplier and is used to monitor and measure the delivery of the requirements. It is also used to cross reference invoicing against delivery.

The rights, obligations and details agreed and set out in each SoW, only apply to the Services and Deliverables for this SoW. They do not relate to any past or future SoW, unless specified.

Where applicable, the Buyer and the Supplier may also choose to add the following documents to complement this SoW:

- The initial Service Delivery Plan – developed for this SoW
- Addition documents to support the deliverables
- High level objectives for this SoW

Overview:

SoW start date:	[19/03/2018
SoW Reference:	[CCIS17B82
Buyer:	[IICSA
Supplier:	[Aristi Ltd
Sub-Contractors: <i>(list all sub-contractors)</i>	[N/A
Overall Estimated Service Completion Date: <i>(the "Completion Date")</i>	[18/03/2018
Duration of SoW <i>(How long the SoW will last – expressed as Working Days)</i>	[N/A
Charging Mechanism(s) for this SoW: <i>(Capped/ Time and Materials/ Time and Materials/ Fixed Price/ Milestone deliverables)</i>	Fixed Price

Key Personnel:

The Parties agree that the Key Personnel in respect of the Service Delivery are detailed in the table below.

Table of Key Personnel: Personnel for each work package will be selected from the following:

Name	Role	Details
REDACT	CHECK team leader/project lead	To be defined
REDACT	CHECK team leader	To be defined
REDACT	CHECK team member	To be defined
REDACT	CHECK team member	To be defined

REDACT	Project Manager	To be defined
REDACT	Commercial Contact	To be defined
REDACT	Account Manager	To be defined

Deliverables:

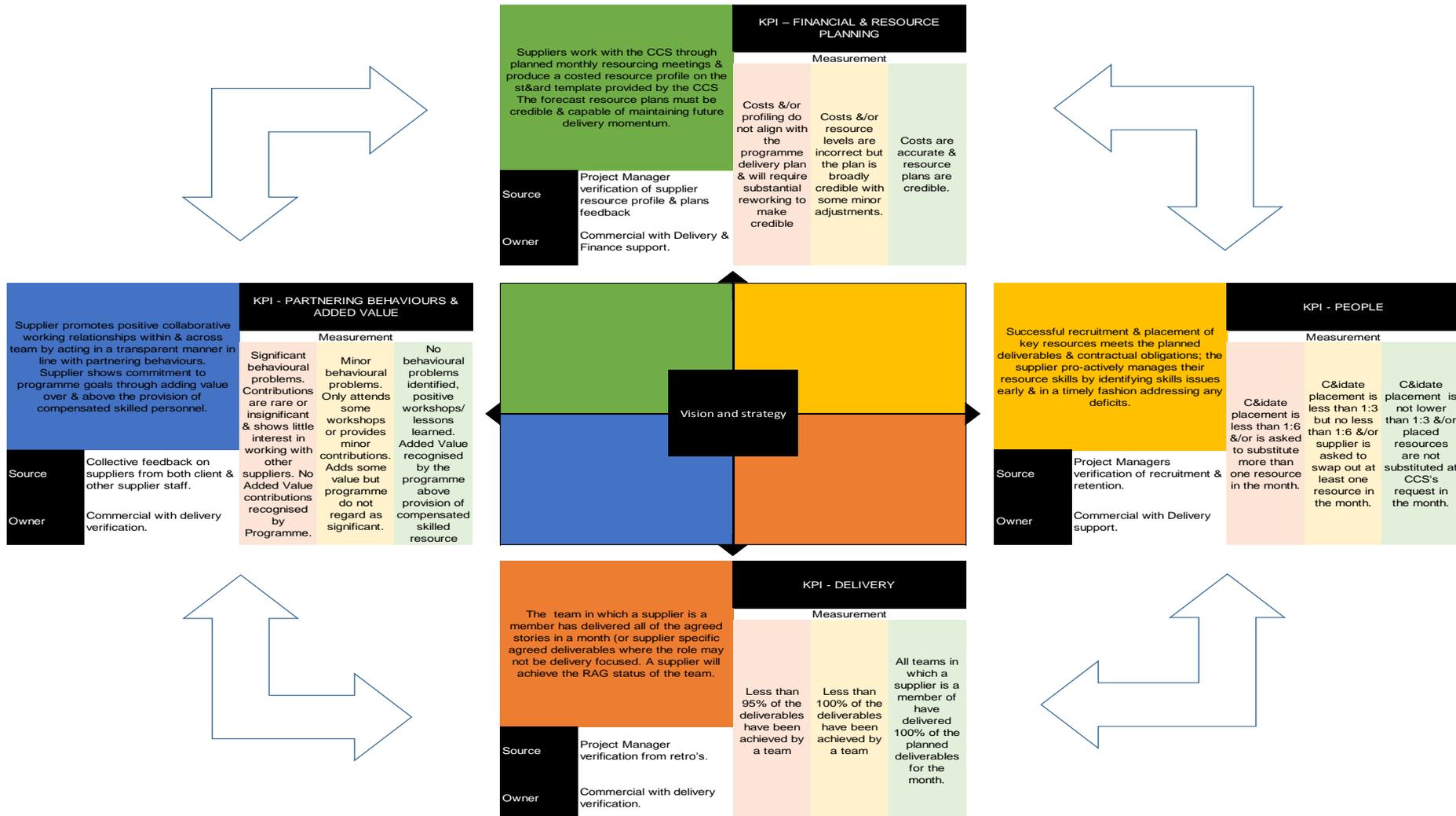
- None defined, these will be defined within each work package during the initial engagement phase.
- Enter Deliverables.

Additional Requirements

None defined, these will be defined within each work package during the initial engagement phase

Balanced scorecard & KPIs:

In addition to the Supplier's performance management obligations set out in the framework agreement, the Buyer and the Supplier have agreed the following Balanced Scorecard & KPIs for this Release: (use this template and amend with your own measures in line with these headings) Copy of the below can be found [here](#)



Contract Charges:

The Maximum Price for this SoW is: £xxxxx |

The preferred charging mechanism for this SoW is: *(Please tick below)*

- CAPPED TIME AND MATERIALS (complete Time and Materials table)
- TIME AND MATERIALS (complete table below)
- FIXED PRICE (complete table below)
- MILESTONE DELIVERABLES

The detail behind each charging mechanism is found below.

Capped Time and Materials

- The maximum price the Supplier is entitled to charge the Buyer for Services delivered on a Capped Time and Materials basis (excluding VAT but including Expenses) is known as the Maximum Contract Charges.
- The Buyer must specify if the Maximum Price for this SoW and stipulate the Service Period. E.g. Maximum Price per Week, per Working Days etc.
- Capped Time and Materials shall be calculated on a daily basis at the respective time and material rates for each Supplier Staff for every day, or pro rata for every part of a day, that the Supplier Staff are actively performing the Services and in accordance with the relevant rates for such Supplier Staff as required to perform such Services.
- The Supplier acknowledges and agrees that it shall provide the Services in relation to this SoW within the Maximum Price set out above; and it shall continue at its own cost and expense to provide the Services, even where the price of Services delivered to the Buyer on a Capped Time and Materials basis has exceeded the Maximum Price.
- The Buyer shall have no obligation or liability to pay for the cost of any Services delivered in respect of this SoW after the Maximum Price has been exceeded.

Time and Materials (T&M)

- The T&M pricing structure shall apply:
 - ✓ for Services delivered (or as agreed otherwise by the Parties); and
 - ✓ for other aspects of the Services as may be agreed by the Parties.
- T&M shall be calculated:
 - on a daily basis at the respective T&M rates for each Supplier Staff, for every day,
 - or pro rata for every part of a day that the Supplier Staff are actively performing the Services
- The relevant rates for such Supplier Staff is set out in the table below.
- The Supplier shall provide a detailed breakdown of any T&M; with sufficient detail to enable the Buyer to verify the accuracy of the T&M Contract Charges incurred.
- For the avoidance of doubt, no risks or contingencies shall be included in the Contract Charges in addition to the T&M.
- The Supplier shall retain a record timesheet for all staff providing the Services; which the Buyer may request for inspection at all reasonable times on request.
- T&M rates (excluding VAT) is an estimated cost for a SoW from Supplier proposal. If additional work is required. A further SoW is required. The Maximum Contract Charges may not be exceeded without consent from the Buyer. Please refer to Contract Change Note.

Experience Level/ Day Rate/planned duration for this SoW

Cyber Security Roles	Practioner Day Rate £	Planned Duration No. of Days	Senior Practioner Day Rate £	Planned Duration No. of Days	Lead Practioner Day Rate £	Planned Duration No. of Days	Total
Total value of this SoW:							
Estimated Contract Charge: (23. of the Order Form)							
Remainder of value under Estimated Contract Charge: (23. of the Order Form minus All SoW total values)							
Is there any risk to exceed Estimated Contract Charge: Y/N & Comments below.							Choose an item.
Comments: This is not yet defined, it will be clarified within each work package during the initial engagement phase							

Fixed Price

- Where Services for this SoW are being delivered on a Fixed Price basis, the Contract Charges set out in the table below shall apply.
- The Parties acknowledge and agree that the following assumptions, representations shall apply in relation to the prices set out in the table below.
- Fixed Price Contract Charges (excluding VAT) shall be applied as follows:

Fixed Charge	Description	Service Period (or if Payment linked to Milestones then, Milestone Date)	Breakdown By Role and Duration
REDACT	Check Team Leader - Infrastructure	N/A	Per day
REDACT	Check Team Leader- Web Aps	N/A	Per day
REDACT	Check Team Leader Web Aps including T&S	N/A	Per day
REDACT	Chck Team Member	N/A	Per day

Milestone Deliverables

- Milestone Deliverable pricing shall be against the service delivery plan agreed by the Buyer and Supplier at the start of the SoW.
- The Supplier must complete the service Deliverable by the due date.
- The Buyer will review the Deliverable against the agreed acceptance criteria to sign off acceptance
- Once the Buyer has accepted the Deliverable the Supplier can raise and send an invoice.

Agreement of SoW:

By signing this SoW, the Parties agree to be bound by the RM3764ii Call-Off Contract terms and conditions set out herein:

Signed by an authorised signatory for and on behalf of the Buyer and the Supplier

• **SIGNED:**

	Supplier:	Buyer: Sam Chowdhury
Name:	REDACT	REDACT
Title:		
Signature:	REDACT	REDACT

Please send copies of all SoW to Crown Commercial Service email:
Cloud_Digital@crowncommercial.gov.uk titled Cyber Security Services 2 SoW.

SCHEDULE 6 - CONTRACT CHANGE NOTE

Call-Off Contract reference: [Insert]

Contract Change note variation number: [Insert]

This amendment to the agreement is between:

the “Buyer”

[Buyer Full Name

Buyer Full Address]

the “Supplier”

[Supplier Full Name]

[Supplier No.]

[Supplier Full Address](registered office address)

The variation:

The Contract is varied as follows and shall take effect on the date signed by both Parties:

Full Details of the proposed change:

[Insert]

Reason for the change:

[Insert]

Likely impact, if any, of the change on other aspects of the Contract:

[Insert]

Words and expressions in this Contract Change Note shall have the meanings given to them in the Contract.

The Contract, including any previous changes shall remain effective and unaltered except as amended by this change.

Signed by an authorised signatory for and on behalf of the Buyer and the Supplier

SIGNED:

	Supplier:	Buyer:
Name:	[]	[]
Title:	[]	[]
Signature:	<p>X _____</p> <p>Select date]</p>	<p>X _____</p> <p>Select Data]</p>

PART C – RM3764ii Standard Terms

The standard terms and conditions of the RM3764ii Call-Off Contract have been developed specifically for government/public sector.

These terms are non-variable and can be found on the CCS website:

<http://ccs-agreements.cabinetoffice.gov.uk/contracts/rm3764ii>