



**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:	<i>CQC PSO 197 Digital Penetration Testing</i>
Date sent to supplier:	03/12/2019
Purchase Order Number:	TBC

This agreement is between:

the "Buyer"

CARE QUALITY COMMISSION

151 Buckingham Palace Road, 3rd Floor, London SW1W 9SW

the "Supplier"

NCC Group Security Services Ltd

XYZ Building, 2 Hardman Boulevard, Spinningfields, Manchester, M3 3AQ

Together the "Parties"

Service delivery contact details:

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

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:** 23/12/2019
2. **Length of Contract:** 2 YEARS WITH AN OPTION TO EXTEND FOR A YEAR

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** By email to SBS-W.PAYABLES@NHS.NET
 - 4.2. **Who to send invoices to:** Care Quality Commission, T70 Payables F175, Phoenix House, Topcliffe Lane, Wakefield WF3 1WE
 - 4.3. **Invoice information required: e.g. PO, Project** Purchase Order
5. **Invoice Frequency** Monthly in arrears
6. **Contract Charges** Minimum value of this contract is £761,400 excluding VAT and expenses. detailed Contract Charges are

Area	Job Role	Day Rate (excluding VAT)



Buyer contractual requirements:

- 7. Services required: ***

For the supply of digital testing project ref: CQC PSO 197. The detailed Services required are outlined in Schedule 1 in Part B.

Please note extent of the services exclude hardware devices and/or software products.
- 8. Delivery Location(s)/Premises:**

Please refer to Schedule 1 in Part B
- 9. Relevant convictions:**

Clause 44 of the Call off Terms and Conditions shall apply
- 10. Staff Vetting and Security Clearance:**

Clause 45 of the Call off Terms and Conditions shall apply. Security Check Clearance required
- 11. Local health and safety procedures:**

Refer to the CQC Policy for Health and Safety.
- 12. Non-Disclosure requirements:**

N/A.
- 13. Exit Planning:**

Clause 11 of the Call off Terms and Conditions, and Schedule 5 in Part B shall apply.
- 14. Security Requirements:**
(including details of Security Policy and any additional Buyer security requirements) **

Clause 21 of the Call off Terms and Conditions, and Schedule 9 in Part B shall apply.
- 15. Protection of Buyer Data:**

Clause 40.4 of the Framework Agreement, clause 21 of the Call off Terms and Conditions, Schedule 8 and Schedule 9 in Part B shall apply
- 16. Standards:**

CESG Cyber Security Consultancy Standard
- 17. Business Continuity and Disaster Recovery:**

Clause 17 of the Call off Terms and Conditions, and Schedule 7 in Part B shall apply.
- 18. Insurance:**

Public Liability Insurance – minimum level of cover [REDACTED] for each individual claim

Employment Liability Insurance – minimum level of cover [REDACTED] for each individual claim

Professional Indemnity – minimum level of cover [REDACTED] for each individual claim

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
29	Changes to 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 - ██████████ in each Contract Year in which the default occurred or is occurring • For all other losses, ██████████ or a sum equal to ██████████ depending on the liability damage/loss or impact For loss of Customer Data or Customer Personal Data - ██████████
39.6.1	Termination Events Material Breach	Will remain 15 Working Days
Part B	Schedule 5- Exit Plan	
Part B	Schedule 7 Business continuity and disaster recovery plan	
Part B	Schedule 8- Processing, personal data and data subjects	
Part B	Schedule 9 – Security Requirements	

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

Schedule 1 - Requirement Statements

22. Key Sub-Contractors

No sub-contractors will be used

23. Contract Charges

Area	Job Role	Day Rate (excluding VAT)

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:	Buyer:
Name:		
Title:		
Signature:		

PART B – THE SCHEDULES

SCHEDULE 1 – THE BUYER NEEDS, YOUR OFFER & YOUR PRICES

RM3764ii Cyber Security Services

Care Quality Commission
Penetration Testing

The Buyer Needs

GUIDE TO MINI COMPETITION DOCUMENTS

Name	About
The Buyer Needs	Outline of the buyer's requirement (this document)
Your Offer	Complete and submit this template on how you can deliver this requirement
Your Prices	Complete and submit this template with your prices and discounts Please note it is a mandatory requirement to submit your rate card for information for any future requirements throughout the contract. This will not be used for scoring.
Call-Off Contract Parts A&B	Buyer specific terms and conditions
Call-Off Contract Part C	Standard terms and conditions (non-variable)

MINI COMPETITION KEY DATES

Publish Date	4 October 2019
Deadline for asking question	12:00 on 18 October 2019
Closing date for bids	16:00 on 22 October 2019

1. REQUIREMENT FACT FILE

Project Lead:	
Buyer:	Care Quality Commission
Delivery Location:	Remote locations allowed, although office locations are in Newcastle upon Tyne and London
Charging Mechanism:	Day rates via the Statement of Work in Schedule 4
Latest Start Date:	1st December 2019
Expected Contract Length:	2 years with an option to extend for a year

2. THE REQUIREMENT

2.1 SUMMARY OF THE REQUIREMENT

Purpose of the requirement

- For the Care Quality Commission (CQC) to meet the aims of our current strategy and deliver a more efficient operating model we are undertaking a transformation programme that is Digitally focused and Intelligence led.
- This programme of work has started in 2017-18 and will run through to 2020-21 and will see CQC invest more than £30m over this period funded through our capital allocation and existing revenue budgets, providing a return on investment that enables CQC to meet existing spending review targets.
- This work is therefore vital to ensure that investments planned as part of our transformation programme provide value for money, deliver to planned timescales and realise the benefits as set out in each business case.
- New CQC systems and services will not be allowed to go live without having penetration (vulnerability) testing and performance (load) testing performed to ensure they are secure and comply with non-functional specifications.
- The call off nature will ensure we only spend what is required when a system and services is ready for testing. The indicative whole life costing envelope for this contract is £1,240,000 - £1,250,000 (including vat). However, this will be used on a project by project basis throughout the life of the contract. The overall value will be monitored against a range of project requests.
- The scope of this contact will cover a range of system and services that are critical to the value of CQC and the testing required will seek to identify any vulnerability and security assessments that will have a significant impact on the CQCs reputation and values. The supplier will provide specialist application and infrastructure security testing.

Overview of the Requirement

- An agreement is required to cover cloud based, penetration testing services that will ensure any new hosting agreements are safe, secure and that security is not compromised. These are specialist skills and Care Quality Commission do not have internal resources with the skills or knowledge required to deliver this service.

- It is not possible, affordable or practical for Care Quality Commission to staff the organisation with these specialist resources. A Statement of Work ("SoW") under the Call-off contract will be used only when required and the set rates used will be monitored and controlled.
- New Care Quality Commission systems and services will not be allowed to go live without having penetration (vulnerability) testing and performance (load) testing performed to ensure they are secure and comply with functional and non-functional specifications.
- As systems are migrated away to cloud solutions, assurance of their vulnerability and performance risk will not be possible and therefore Care Quality Commission will be exposed to unacceptable levels of risk. Examples of risk that require protection against are cyber-attacks, data breaches, disclosure of confidential and personal information such as patient identifiable data and denial of services attacks either via applications or the infrastructure that they are hosted on.
- As CQC develop new systems and services to support the strategy it will require penetration (vulnerability) testing and performance (load) testing to be performed on a repeated basis, as we focus on developing new internet facing services. The requirement covers any new or significantly changed (i.e. a new interface) service with an internet facing element that will generally require a penetration test of both the application and its infrastructure. Anything cloud hosted will require application and infrastructure penetration testing and any new or significantly amended service will require a performance or load test against its Non-Functional Requirements for throughput and speed.
- This work will enable CQC to deliver new Digital services and intelligence led regulation with low risk and at pace.
- CQC will be developing a series of new systems to enable organisational strategy. The development and delivery of the strategy will require detailed understanding of CQC systems, infrastructure and endpoints. It is imperative that new services operate according to standard best practice approaches and are created in anticipation of constant and rapid change.
- Furthermore, as CQC transitions existing Digital services away from on premise solutions managed by the Atos IMS3 contract or Computacenter to cloud hosted solutions such as Microsoft Azure and Oracle Cloud, it's imperative that each application or infrastructure component is independently tested for Security and Performance and any vulnerabilities or issues scanned, highlighted and addressed accordingly.

Key Deliverables/Required Deliverables

- Performance testing (i.e. evaluation of the quality, speed, scalability and capability of a product);
- Application security testing (i.e. evaluation of software, hardware, and procedural methods to protect applications from external threats);
- Infrastructure security testing (e.g. penetration testing to evaluate the security of a computer system or network by simulating an attack from a malicious source) against several IT delivery projects we currently have planned in our programme of work.
- Both Black Box and White Box Testing

The Scope of the requirement

The scope of requirement would be seeking assessments that identify and manage any existing vulnerabilities as well as ensuring the correct security controls are in place.

Examples of the CQC digital initiatives being developed are estimated below, however this is a requirement that is evolving significantly with the ongoing CQC digital transformation strategy and as such cannot be guaranteed.

Digital Initiative	Performance testing	Application security testing	Infrastructure security testing
Registration			
PMS PIR			
SYE			
Intranet			
Hospitals PIR			
Evidence mgmt.			
Data sharing			
Automation			
Data lake			
Visualisation tools			
Cloud migration OBIEE			
Cloud migration OBDD			
ETL rewrite/migration			
Authoring and Pub			
Device upgrade			
MS365			
Infrastructure improvements			
FSP			
MHA DB changes			
CC/storm integration			
Cygnus P3			
Total Days			

Key Performance Indicators

Indicator	Measured by
Testing Scoping Report	Receipt of report
Testing Phase 1	Testing confirmation within agreed time parameters
Testing Phase 2	Testing confirmation within agreed time parameters
Testing Outcomes including vulnerability assessment	Receipt of report

Out of Scope

- Software licensing

2.2 REQUIREMENT BACKGROUND

CQC: Who we are

The Care Quality Commission is the independent regulator of health and adult social care in England. We make sure that health and social care services provide people with safe, effective, compassionate, high-quality care and we encourage services to improve.

In Summary our role is to:

- Register health and adult social care providers
- Monitor and inspect services to see whether they are safe, effective, caring, responsive and well-led, and we publish what we find, including quality ratings
- Use our legal powers to act where we identify poor care
- Speak independently, publishing regional and national views of the major quality issues in health and social care, and encouraging improvement by highlighting good practice

CQC: Our Strategy 2016 – 2021

Our strategy has been developed based on what thousands of people, providers, staff and partners have told us and what we have learned from more than 22,000 inspections. It sets out an ambitious future for a more targeted, responsive and collaborative approach to regulation, so more people get high quality care.

You can download the full strategy from our public website at www.cqc.org.uk/content/our-strategy-2016-2021.

The years ahead are an exciting period to make this strategy a reality, working closely with people who use services, the providers we regulate and our national and local partners to develop a regulatory approach relevant and appropriate for fast changing health and adult social care services in England.

Background

CQC will make substantial investment in the next two years in improving the digital services that providers of health and care services and members of the public use to engage with us. We will also invest in the enabling technology that underpins those services and our core business. This investment is focussed on the following outcomes;

Making CQC an even more effective regulator of health and adult social care:

Reshaping the inspection model, to focus more effort on identified risk by combining and mining information collected from the public, from providers, by our inspectors and from other sources, including concerns and whistleblowing, to generate rapid insight and action.

Making CQC easier to work with: Using 'always on' digital channels to collect information from providers, asking only for information we do not hold and asking in a way that makes it easy for them to get it right first time whether in registration, inspection or other interactions.

Making it easier for our staff to do their jobs: With the right devices and information access to operate effectively as a remote workforce. Keeping staff close to providers while remaining fully connected to the CQC, both practically and emotionally.

Making sure people understand our information: By relaying the right information to the right people through the right channel at the right time. Audience specific communication will lie at the heart of all report and information publication.

2.3 ESSENTIAL SKILLS AND EXPERIENCE

The supplier should have the following skills:

1. The supplier must be CREST accredited.
2. Suppliers must be able to demonstrate the scale of their penetration testing; application security testing and Infrastructure security testing services.
3. Supplier must be able to demonstrate the scope of their available penetration testing; application security testing and Infrastructure security testing services, identifying, with examples of practice, the layers in the 7- layer ISO model that they operate at.
4. Supplier must be able to demonstrate where they have undertaken penetration testing; application security testing and Infrastructure security testing.
5. Supplier must be able to provide CVs for the staff who would undertake penetration testing; application security testing and Infrastructure security testing for CQC, with their SFIA level (The Skills Framework for the Information Age model for describing and managing competencies for ICT professionals). There is a requirement to ensure that testing staff are all security cleared.
6. Supplier must be able to describe their organisations' approach to information security along with any security accreditations that they hold.
7. Supplier must be able to describe their approach to carrying out penetration testing; application security testing and Infrastructure security testing, including references to any relevant industry frameworks.
8. Supplier must be able to describe their plan for carrying out this penetration testing; application security testing and Infrastructure security testing and any access to, or time that they will need from CQC staff or the 3rd party organisations that manage the endpoints.
9. Supplier must be able to provide an example report that they will provide to CQC as the output resulting from the penetration testing; application security testing and Infrastructure security testing. It is preferred that this be a real report and acknowledged that this will therefore need to be anonymised.
10. Suppliers will be required to sign a non-disclosure agreement.

2.4 OBJECTIVES AND DELIVERABLES

The contract will be in place for two years to support the modernisation of CQC systems and to provide the assurance that services migrated to the Cloud have not inadvertently introduced any security vulnerabilities. The requirements are;

- Performance testing (i.e. evaluation of the quality, speed, scalability and capability of a product);
- Application security testing (i.e. evaluation of software, hardware, and procedural methods to protect applications from external threats);
- Infrastructure security testing (e.g. penetration testing to evaluate the security of a computer system or network by simulating an attack from a malicious source) against several IT delivery projects we currently have planned in our programme of work.
- Black box and white box testing.

The scope of testing will be presented by CQC to the supplier as part of a planned project plan. It will be important to produce a plan that demonstrates the required testing. It will be scheduled within an agreed timeframe. A report will be prepared that provides a methodology for the project, including initiation, test planning and establish the goals and objectives based around risk. The approach will be summarised, and the results should be analysed, and high-risk issues will be reported immediately to CQC.

A report appropriately encrypted will be issued to CQC once the testing is completed. Reporting via an online portal would be preferred and should seek to identify generic vulnerability and current threat overview. A final report outlining the results of the testing and advice and guidance on improving the necessary security controls is required.

CQC are seeking continuous cycle of testing, remediation and ongoing monitoring.

3. LOTS & STRUCTURE

3.1 The required Cyber Security Services are:

LOT 1: Certified Cyber Consultancy	✓ LOT 2: Penetration Testing CHECK
<input type="checkbox"/> 1.1 Risk Assessment	
<input type="checkbox"/> 1.2 Risk Management	<input type="checkbox"/> LOT 3: Cyber Incidents (CIR)
<input type="checkbox"/> 1.3 Security Architecture	
<input type="checkbox"/> 1.4 Audit and Review	<input type="checkbox"/> LOT 4: Tailored Evaluations (CTAS)
<input type="checkbox"/> 1.5 Incident Management	

NB. As a supplier, you must have a valid NCSC certification in the required lot before you can bid to provide services in that lot

4. TIMESCALES AND LOGISTICS

4.1 Key Project Timescales

It is expected that this contract will cover several products and services that are being developed within CQC. The testing will be arranged, locations agreed, and dates planned to a schedule.

4.2 Delivery Logistics

Location(s) where work will be carried out	Remote location is available, although the main CQC Offices are in London and Newcastle upon Tyne
Working arrangements	To be arranged prior to the work being scoped
Security Clearance Requirements	Minimum requirement is Security Check clearance
Start Date	1 st December 2019
Expected completion date	2 years with an option to extend for a year

4.3 Provisional mini competition timeline

DATE	ACTIVITY
4/10/19	Requirement Published
18/10/19	Deadline for asking questions Please submit all clarification questions by 12:00hrs Please note that we aim to publish all response to Q&A within 24hrs
22/10/19	Closing date for applications Potential Provider must upload submission to the eSourcing tool by 16:00hrs.
5/11/19	Award Notification Publish Successful and un-successful Potential Suppliers.
1/12/19	Expected Start Date

5. HOW WILL MY BID BE EVALUATED?

Evaluation criteria will follow the approach below:

Written submission (Quality)	80%
Price (Financial)	20%
Total	100%

The objective of the selection process is to assess the responses and then select a preferred bidder.

The Scoring Methodology for the written submission (Quality) will be awarded in accordance with the below Scoring Matrix:

Grade label	Grade	Definition of grade
Excellent	4	The Supplier's proposal evidences significant levels of understanding and offers an innovative solution that includes desirable value-add to the Authority.
Good	3	The Supplier's proposal has evidenced a level of understanding that assures there will be desirable value-add within the solution or superior and desirable (time or quality) delivery outcomes.
Satisfactory	2	The Supplier's proposal has a suitable level of detail to assure that a satisfactory delivery of the service requirement is likely.
Weak	1	The Supplier's proposal has merit, although there is weakness (or inconsistency) as to the full satisfaction of the delivery requirement
Unacceptable	0	The response has been omitted, or the Supplier's proposal evidences inadequate (or insufficient) delivery of the requirement

Price (Financial)	20%
<p>Your pricing and discounts for the delivering the Buyer's Needs are submitted in the 'Your Prices' template. This section will count for 20% of your overall evaluation score. Only if you meet the minimum pass marks of a 2 in all of the evaluation criteria in the previous parts of 'Your Offer' will your prices be evaluated.</p> <p>Price will be assessed by the maximum points of 20% being awarded to the lowest price as per the calculation below. The Price evaluation will be taken from the cell I30 in 'Your prices' and is the Discounted Estimated Total Cost.</p> <p>Score = $\frac{\text{Discounted estimated total cost}^*}{\text{Tender Price}} \times 20\% \text{ (maximum mark available)}$</p> <p>* Discounted estimated total cost is Cell I30 in 'Your Prices'.</p> <p>CQC will award the Contract to the Supplier submitting the most economically advantageous tender (i.e. the Tender that achieves the highest combined final score (out of 100%), made up from Your Offer score (maximum score = 80) and Your Prices (maximum score = 20). In the event that two or more Suppliers obtain the same highest combined final score, the Supplier with the highest score for the 'Financial' element will be deemed the winner and awarded the Contract.</p> <p>Please note it is a mandatory requirement to submit your rate card for information for any future requirements throughout the contract. This will not be used for scoring.</p>	

Suppliers must outline their plan for delivering CQC's requirement according to the guidance set out in this section. Should your response be successful in this Further Competition, your submission may form part of the Call-Off Agreement.

There are 4 requirement statements in total. Suppliers are required to respond to all of the questions below. Questions should be answered in full and should not refer to other documents or appendices. Suppliers are referred to the document 'Your Buyer Needs' and reminded that evaluation of their requirement statements will account for 80% of their total tender score.

Please answer the questions below as fully as possible, taking note of the marks available. You must score a 2 or above in all of the below evaluation criteria to be considered for this contract.

Your response is to be separately evaluated. The evaluation criterion is set out as a standalone item. Each separate evaluation criterion response will be evaluated in its entirety, clearly separate from any other evaluation criterion response that the supplier elects to submit for evaluation. Failure to provide a response will result in your organisation scoring no marks for that question. For the avoidance of doubt, evaluators will not cross reference information from one question to another question regardless of its relevance or quality.

Any information provided which is not referenced or exceeds any specified word count will not be evaluated. Please submit the document in this word document format (.doc) NOT as a PDF. Hyperlinks and embedded documents will not be considered. Please note each question limit, using Arial 12 point, single spaced font. Any material provided over this stated limit will not be evaluated. DO NOT include any additional appendices, brochures or other marketing materials to supplement your tender response.

Please refer to the 'Your Offer' document for more information about each evaluation stage.

- The response for hypothetical test case will be scored for quality using the approach and methodology you outline in the Your Offer document. The pricing breakdown for this hypothetical test case should be included into the mini-competition document - Your Prices.xlsx. and should be used to demonstrate the price and rates you would charge. Please note it is a mandatory requirement to submit your rate card for information for any future requirements throughout the contract. This will not be used for scoring.

CQC will award the Contract to the Supplier submitting the most economically advantageous tender (i.e. the Tender that achieves the highest combined final score (out of 100%), made up from Your Offer score (maximum score = 80) and Your Prices (maximum score = 20). In the event that two or more Suppliers obtain the same highest combined final score, the Supplier with the highest score for the 'Financial' element will be deemed the winner and awarded the Contract.

6. GOVERNANCE, TERMS AND CONDITIONS

6.1 Governance

Regular meetings with CQC and the supplier will be set up once the contract is awarded. This will review the work plan, timings, costs, spends and answer any queries. A quarterly report will be produced by the supplier detailing engagements carried out during the period, number of days effort expended and number of invoices, including total spend, drawn down on the contract. This report should also summarise any significant findings made, and threats detected during testing carried out in the reporting period. The reports will be timed to precede the regular meeting between the CQC contract manager and the supplier.

Contract Management Arrangement

Buyer's Responsibilities

- Appoint a representative from the CQC Digital Team to act as the contract manager.
- Provide all necessary information to undertake testing.
- Be available to discuss testing outcomes, any potential scenario testing should it be necessary and any changes in scope should they be required.
- Ensure payment is made promptly in line with the contract.

Task	Customer Roles In CQC	Comment
1. Define requirements	Project/Product Manager	Collaborate with the supplier.
2. Governance and approval	Business Contract Owner	Co-ordinating all contract activity within 5 days
3. Complete Statement of Work	Project/Product Manager	Statement of Work Agreed and signed. Supplier sends signed copy back to DM
4. Arrange for SoW sign off by CQC	Project/Product Manager	DM sends SoW for sign off in line with Scheme of Delegation
5. Copy of SoW to Commercial	Project/Product Manager	Copy to Commercial
6. Raise requisition	Digital Commercial Officer	Requisition raised with the contract order form

Suppliers Responsibilities

- Provide a single point of contact to manage the relationship with CQC.
- Provide a scoping report that outlines testing requirements, the plan for testing and timeframes. This will include the identification of meeting points that they will initiate and attend.
- Produce a final report detailing testing, results and advice to improve security controls if required.

6.2 Terms and Conditions

Subcontracting Permitted? <i>Supplier must be certified in all the required services, but may subcontract to supplement their resources if required</i>	No
Partnering Permitted? <i>Suppliers who are not certified in all the required services, but wish to bid for all, may partner with another Supplier(s) on the framework who have been certified in that service</i>	No

Buyer specific Terms and Conditions apply to this agreement. These can be found under **Call-Off Contract Part A&B**

These Buyer specific terms will supersede the standard terms within **Call-Off Contract Part C**

Your Offer

WHAT MAKES UP 'YOUR OFFER'?

PART 1 SUPPLIER CONFIRMATION

Pass/Fail:

You **must** pass all three supplier confirmation questions for your bid to be considered

PART 2 WRITTEN SUBMISSION

Outline your plan for delivering the Buyer's requirement according to the guidance set out in this section.

Should your response be successful in this Further Competition, your submission may form part of the Call-Off Agreement.

As specified in 'The Buyer Needs' this section will count for 80% of your overall evaluation score.

PART 3 YOUR PRICES

Once you have completed 'Your Offer' (this document) please refer to the 'Your Prices' template for guidance on how to submit your pricing and discounts for delivering the Buyer's Needs.

As specified in 'The Buyer Needs' this section will count for 20% of your overall evaluation score.

Only if you meet the minimum pass marks of a 2 in all of the evaluation criteria in the previous parts of 'Your Offer' will your prices be evaluated.

Price will be assessed by the maximum points of 20% being awarded to the lowest price as per the calculation below. The Price evaluation will be taken from the cell I30 in Your prices and is the Discounted Estimated Total Cost.

Score = Discounted estimated total cost* x 20% (maximum mark available)

Tender Price

* Discounted estimated total cost is Cell I30 in 'Your Prices'.

CQC will award the Contract to the Supplier submitting the most economically advantageous tender (i.e. the Tender that achieves the highest combined final score (out of 100%), made up from Your Offer score (maximum score = 80) and Your Prices (maximum score = 20). In the event that two or more Suppliers obtain the same highest combined final score, the Supplier with the highest score for the 'Financial' element will be deemed the winner and awarded the Contract.

Please note it is a mandatory requirement to submit your rate card for information for any future requirements throughout the contract. This will not be used for scoring.

PART 1: SUPPLIER CONFIRMATION

1. Availability
2. Security Clearance
3. Subcontracting/Partnering

QUESTION:

AVAILABILITY

Minimum Pass Mark:

PASS

Fail No confirmation - services will not be available at the required location(s) or within the required timeframe

Pass Confirmation all services available/deliverable at the required location(s) within required timeframe

YOUR RESPONSE

I confirm that NCC Group Security Services Limited is available at the required location(s) and between the dates specified by the Buyer in 'The Buyer Needs'.

PART 1: SUPPLIER CONFIRMATION

QUESTION:

SECURITY CLEARANCE [Security Check]

Please confirm whether your proposed delivery team members have successfully completed the staff vetting required OR confirm that you are willing to undertake the required Staff Vetting prior to commencing work on site.

The Buyer confirms that they will sponsor the relevant security clearance to enable the supplier to complete the work.

Minimum Pass Mark: PASS

Fail Information supplied is missing or incomplete

Pass

Staff Vetting and security clearance with date has been provided for all proposed staff OR confirmation that this will be carried out prior to commencing work on site as date indicated in the requirements.

YOUR RESPONSE

All NCC Group CHECK staff are cleared to at least SC level (facilitating unsupervised access to OFFICIAL SENSITIVE information) with a large number of the team having additional higher clearances. However, please note that NCC Group cannot detail the names of the delivery team at this stage, as we only schedule resources when the type of assessment, location and dates are agreed with you. We can confirm that once work is scheduled and agreed with you, we are willing to undertake any additional required Staff Vetting.

Full Name of individual proposed:

Is the Required Staff Vetting complete? Yes/No

Date Checked by Supplier: Date Valid Until:

Other UK Government Security Clearances Held:

Disclaimer, We agree to carry out the required Staff Vetting post award and prior to commencing work on site

Yes/No

Unknown at the point of writing response but all consultants go through staff vetting and all will have SC and most will have DV

Yes

Your Offer

1. Availability
2. Security Clearance
3. Subcontracting/Partnering

Your Offer

Page 6 of 17 CYBER SECURITY SERVICES RM3764ii

PART 1: SUPPLIER CONFIRMATION

1. Availability
2. Security Clearance
3. Subcontracting/Partnering

QUESTION:

SUBCONTRACTING/PARTNERING

Not applicable. No Subcontracting is allowed.

NCC Group will not be using subcontractors or third parties to deliver any of the services described within this ITT.

PART 2: WRITTEN SUBMISSION

Name of Supplier: NCC Group Security Services Limited

This written submission contains the response form for completion by the supplier and will be returned to Care Quality Commission via the Bravo eSourcing portal.

The Scoring Methodology for the written submission (Quality) will be awarded in accordance with the below Scoring Matrix:

Grade label Grade Definition of grade

Excellent 4 The Supplier's proposal evidences significant levels of understanding and offers an innovative solution that includes desirable value-add to the Authority.

Good 3 The Supplier's proposal has evidenced a level of understanding that assures there will be desirable value-add within the solution or superior and desirable (time or quality) delivery outcomes.

Satisfactory 2 The Supplier's proposal has a suitable level of detail to assure that a satisfactory delivery of the service requirement is likely.

Weak 1 The Supplier's proposal has merit, although there is weakness (or inconsistency) as to the full satisfaction of the delivery requirement

Unacceptable 0 The response has been omitted, or the Supplier's proposal evidences inadequate (or insufficient) delivery of the requirement

Suppliers must outline their submission for delivering CQC's requirement 'The Buyers Needs', according to the guidance set out in this section. Should your response be successful in this Further Competition, your submission may form part of the Call-Off Agreement.

Within the Written Submission, there are 4 requirement statements in total. Suppliers are required to respond to all of these questions below. Questions should be answered in full and should not refer to other documents or appendices. Suppliers are referred to the document 'Your Buyer Needs' and reminded that evaluation of their requirement statements will account for 80% of their total tender score.

Please answer the questions below as fully as possible, taking note of the marks available. You must score a 2 or above in all of the below evaluation criteria to be considered for this contract. Your response is to be separately evaluated. The evaluation criterion is set out as a standalone item. Each separate evaluation criterion response will be evaluated in its entirety, clearly separate from any other evaluation criterion response that the supplier elects to submit for evaluation. Failure to provide a response will result in your organisation scoring no marks for that question. For the avoidance of doubt, evaluators will not cross reference information from one question to another question regardless of its relevance or quality.

Any information provided which is not referenced or exceeds any specified word count will not be evaluated. Please submit your response as part of this word document format NOT as a PDF. Hyperlinks and embedded documents will not be considered. Please note each question limit, using Arial 12 point, single spaced font. Any material provided over this stated limit will not be evaluated. DO NOT include and additional appendices, brochures or other marketing materials to supplement your tender response.

Requirement Statements

1. The object of the testing is to provide a number of assessments, specific to the testing type, in report form that will include, where applicable:

- Any security issues uncovered
- Details the scope of testing undertaken
- An assessment by the test team as to the level of risk that each vulnerability exposes the organisation or system to
- Recommendations for resolving each issue found

Please tell us how you would deliver the requirement outlined in 'The Buyer Needs'. This submission should include, but not be limited to, details of;

- How you will approach and plan for the requirements
- Previous experience you have delivering similar projects
- The expertise, roles and structure of your proposed team
- How your team will work with the buyer (integrating and collaborating with existing teams, how you intend to report etc)
- How your proposal will deliver value for money by optimising costs, generating savings and delivering quality

You should refer back to 'The Buyer Needs' throughout your proposal.

WordCount: No more than 2 A4 sheets of paper and font size of Arial 12 in this word document (.doc)

Question Weighting: 25%

2. Comment and confirm if you can provide the following areas of testing

- Vulnerability scanning
- Penetration Testing / ITHC, external and internal (unauthenticated and authenticated)
- Criteria for functional, security and performance application testing (including mobile apps)
- Test automation where applicable
- Hardware (server, firewall and network devices) testing
- Cyber Essentials assessments and tests
- Accessibility testing
- Black and White Box Testing

Please add any other area of testing you can provide which is not mentioned above. Demonstrate the capacity and ability to carry out these range of testing

You should refer back to 'The Buyer Needs' throughout your proposal

Word Count: No more than 1 A4 sheets of paper and font size of Arial 12 in this word document (.doc)

Question Weighting: 15%

3. Please provide a brief description of your approach and methodology for a **hypothetical test case**. The response will be scored for quality using the approach and methodology you outline. The pricing breakdown for this hypothetical test case should be included into the tender document - Your Prices.xlsx. and should demonstrate the price and rates you would charge. This will give a Discounted estimated total cost (Cell I30). Please note it is a mandatory requirement to submit your rate card for information for any future requirements throughout the contract. This will not be used for scoring.

Hypothetical test case

An application has been built and is hosted on a cloud based PaaS / IaaS. The application build has utilised a number of open source software libraries and will interface over secured internet communications with an internal (on premise) active directory and sql database. Once operational the system will provide services to and gather information from a larger number (C. 50,000) of

external users via secured web interfaces available on the company website and may also interface with a cloud based IDAM system.

To evaluate the quality of your response to the hypothetical test you should describe your approach and methodology and we would expect a clear outline of:

- The technical boundaries of the test*
- The types of test expected*
- The timeframe and the amount of effort necessary to deliver the testing*
- What is needed from us to undertake the testing*
- Any compliance or legislative requirements that the testing plan must meet*
- Reporting requirements*
- Agreed timescales for delivery*
- A breakdown of the roles used in this testing including a summary of the standard and calibre of the candidate you are supplying for this testing.*

Please use the Your Prices worksheet to detail the prices and rates you would charge for this requirement.

You should refer back to 'The Buyer Needs' throughout your proposal

Word Count:

No more than 2 A4 sheets of paper and font size of Arial 12 in this word document (.doc)

Question Weighting: 30%

4. Please confirm and respond to the following statements;

- Your organisation has the competence and ability to deliver these testing requirements?*
- When are you able to commence and your responsiveness to commence tests with lead times for engagement?*

You should refer back to 'The Buyer Needs' throughout your proposal

Word Count: No more than 1 A4 sheets of paper and font size of Arial 12 in this word document (.doc)

Question Weighting: 10%

YOUR RESPONSE

NCC Group Response to Requirement Statement 1

NCC Group is a Green Light Certified CHECK company and has been since the inception of the scheme. NCC have a strong commitment to remain an approved provider, an illustration of that commitment is the fact NCC Group have nearly 100 fully certified CHECK consultants, split between CHECK Team Member (CTM) and CHECK Team Leader (CTL) levels. NCC Group are also a CREST Certified company, with a vast number of both Application and Infrastructure CREST Certified Testers. This should help you understand that the level of experience in delivering CHECK penetration tests is unparalleled. The CHECK scheme mandates a high level of quality throughout the process of a penetration test ranging from the way in which projects are managed to the QA of the report. Our commitment throughout this process is to maintain that high standard of engagement.

All assessments for CQC will be undertaken using CHECK consultants, who work directly as full time employees for NCC Group and have a minimum of SC clearance. In terms of team structure, a CTL will always be assigned to run and conduct the CHECK assessment. Depending on the length of assessment, CTMs may be included in the assessment team to meet the CQC's timelines i.e. to reduce the calendar days taken during an assessment by increasing the number of consultants performing the work. Each consultant provided will be chosen by NCC Group to ensure they have the best level of experience most appropriate to the work being conducted. Where possible, consultants will be reused to ensure more value is obtained by the CQC in terms of the consultant understanding the business requirements and situational context. In order to ensure greater value for money for CQC, we will leverage our tried and tested methodologies to

both assess CQCs cloud configuration itself as well as work efficiently within a cloud environment when assessing deployed resources and utilise remote working where feasible to do so.

Regarding experience in the public sector specifically, we are often the chosen security partner for central government departments. As examples, the Cabinet Office FOXHOUND / ROSA programme utilises us in this fashion and the Home Office (who also have migrated to a cloud infrastructure from on premise agreements) use us for their ITHCs which is circa 870 days testing per year. NCC Group engages with most central government departments and have many multiyear agreements implemented due to the consistently high quality standard of work provided as well as the clear value brought by not simply providing technical testers - the consultants can relate technical issues in a business context and make every effort to contextualise risk appropriately. NCC Group currently service over 1,000 clients in the UK with fully qualified CHECK ITHC testing being conducted at over 70 separate HMG clients in the UK.

When CQC wish to seek independent security advice and assurance, you will be able to contact your account manager directly who will work with your project teams to understand the requirement. This discussion will be supported by technical staff within NCC Group who have experience of penetration testing, typically individuals from the CHECK team. Once the requirements have been understood, a formalised proposal will be created which itemises the activities to be conducted, along with pre-requisites that are needed to ensure the assessment progresses smoothly, in addition to the commercial details. This proposal is then reviewed by CQC and can either be amended in the event requirements change or approved if acceptable to CQC. Upon approval, your account manager will then arrange for the assessment to be scheduled in, in line with your timescale requirements.

Our scheduling team will then draw up a test plan, indicating the dates the assessment could take place on and confirming the locations. If the dates are acceptable to CQC, an authorisation form is then sent across to the CQC point of contact with a confirmation statement that the CHECK staff have been secured for your project. This authorisation form is a necessary administrative step to comply with the Computer Misuse Act (CMA). Once this authorisation form has been signed and returned, the assessment is fully confirmed.

Before the assessment takes place, the point of contact within CQC will be contacted by the CTL who is leading the assessment. This is to both introduce themselves and reconfirm the proposed activities, ensuring that pre-requisites are in place and logistics have been arranged. If the assessment is sufficiently complex then there may be a preparation/briefing day arranged between CQC and NCC. This is where a CTL will attend the CQC location in advance of the ITHC and work through a list of pre-requisites needed to conduct the assessment, to ensure the ITHC runs as smoothly as possible and obtains the greatest level of coverage for CQC. This time will also be used to gather further information about the environment and to allow core concerns from the CQC and any accreditors to be specifically called out and checked within the assessment where possible. This will also allow the factoring in of more detail with regards to the business use cases of the environment which allows for more business logic issues to be identified. It also provides the opportunity for the CTL to comment on wider architectural design concerns, as well as facilitate more accurate triaging of the risks in terms of the severities attached to any issues identified. In terms of deliverables, a full and detailed report will be authored for each assessment, in accordance with CHECK guidelines. This report will feature:

- An executive summary, which can be used by the senior leadership team to gain a qualitative understanding of the threat landscape of the environment. There is also a quantitative element where the number of risks in each identified element are provided, broken down by severity.
- A detailed findings section, which provides understandable write-ups for each issue identified and any affected components, providing comments on the risks and individual severity ratings.
- Targeted and actionable remediation guidance for each individual issue identified.
- A full list of methodologies that were worked through during the assessment.

During the assessment, regular wash-up meetings will be held where progress and the observed issues will be commented upon. This will allow CQC to comment on issues and potentially assist

with diagnosis as necessary. Using this collaborative approach, CQC will obtain the benefit of early insight into the assessment and, whilst NCC Group will run the assessment on an impartial basis, CQC will have the opportunity to provide background or mitigation commentary on any applicable issues identified.

In addition to the report, an issue matrix will be provided which is in spread sheet form. This issue matrix contains each issue identified, along with the risk rating, description and targeted remediation advice. It also has tracking functionality which allows the remediation teams to use it as a working document to improve the security posture of the environment.

YOUR RESPONSE

NCC Group Response to Requirement Statement 2

We can confirm that all of the testing required in statement two can be carried out by the team at NCC Group with the caveat that the third bullet is only partially available (we do not carry out performance testing). We provide vast amounts of infrastructure level assessments. We have a history of providing realistic attack simulation and not simply running automated tooling. We ensure that everything raised is accurate and no false positives are presented and evaluate the risk fully. This black box approach is often complemented by a white box style assessment, where privileged access is provided the infrastructure to provide the maximum level of assurance in a shorter period of billable time.

NCC Group carry out thousands of web/mobile application and web service assessments each year. We also contribute to industry tooling, such as Burp (an intercepting proxy) add-ons to increase coverage of automated scanners and assist consultants in delving deeper into potential issues. We also look to assist clients with embedding automated tooling during their development pipeline to identify vulnerabilities at source. We are also credited extensively with a number of vulnerabilities which have been discovered in commercial off the shelf applications as well as the underlying web server stack technologies.

NCC Group conducts a large number of build reviews each year, across all forms of OS. These are conducted on end user devices like thin clients to backend servers which can run more unique systems such as scientific Linux and containerised solutions including their orchestrators. We actively contribute to the CIS benchmarks for all operating systems and we are also involved in the creation of the NCSC guidance for end user device hardening across multiple OS's.

To help you understand how we go further than standard penetration testing, as mentioned above, Our ITHCs are tailored to obtain the most appropriate level of assurance in a pragmatic fashion. For example, where feasible we assess solutions at source e.g. instead of build reviewing all hosts we review Ansible and other build solutions that utilise templates/scripts to give an indication of where further investigation may be required.

We have a strong offering on cloud provider security, in terms of understanding the threat landscape applicable when services are transposed into the cloud as well as deep technical understandings of the service offerings themselves e.g. server-less solutions. This is not just limited to the core platforms such as Azure, however, as we have a proven record of accomplishment with the deployment of DevOps infrastructure and applications, often through agile programmes of work. Delving deeper into our approach to agile projects, NCC Group have extensively worked in an agile fashion across both public and private sector. As sprints deploy new or improved functionality our consultancy approach has allowed a targeted assessment to be undertaken with no drop in assurance levels as the consultant has often already assessed previously implemented functionality thus making it an effective mechanism to obtain real security assurance. Given the desire of CQC to move systems to a cloud based environment we feel that this will be of great value.

YOUR RESPONSE

NCC Group Response to Requirement Statement 3

In this hypothetical test requirement, we have assumed that:

- the wider cloud subscription has been reviewed separately
- CQC utilise PaaS inside the cloud so the underlying infrastructure would not be in scope
- no APIs are present and the application is accessed solely through a web browser
- there are 2 user roles in the application, a normal and administrative role

NCC Group propose to undertake a CHECK security assessment of the new application and its supporting environment. This assessment is broken down into the following phases.

2 days at NCC Group Offices - Web Application & Dependencies Including External Infrastructure Assessment

A thorough hands on assessment will be undertaken of the web application. The assessment will be conducted from 3 different perspectives, namely unauthenticated, authenticated (low privilege) and authenticated (high privilege) roles. This will allow for a thorough evaluation of the role based access controls including validating the appropriate horizontal account separation has been enforced. Testing will be driven by OWASP testing methodologies, with automated evaluation tools utilised alongside manual testing to ensure a greater level of assurance. The version and usage of open source libraries will be evaluated. In a similar vein, checks will be undertaken on the way the application is linked back to the on premise Active Directory solution e.g. through ADFS or a service account. A targeted configuration review will be undertaken on the Azure App Service, which is the PaaS solution as well as on the in-cloud IDAM service, Azure Active Directory. Whilst the underlying services themselves are out of scope, this is to ensure that they have been configured appropriately for CQCs use. This review will also entail checking the network security groups in Azure configured to protect the application service. Additionally, an external infrastructure assessment of the application will be undertaken. This will involve enumerating all exposed services, with an aim of identifying all possible entry points into the environment that would be of use to an attacker in terms of exploiting vulnerabilities e.g. through a reliance on outdated or insecurely configured services, such as TLS/SSL based misconfigurations.

Prerequisites:

In order to complete this phase of the assessment, the following will be required:

- URL of the application
- 2 sets of credentials for each user role in the application (user and administrative roles).
- Provision of any additional authentication criteria, such as smart cards / MFA devices etc.
- Provision of any additional data needed to fully utilise the application i.e. valid data to upload.
- Access to the Azure cloud portal, with permissions to inspect the configuration of the applications services, such as the cloud based IDAM solution and the network security groups protecting the application

1 day at CQC Site - Database Review

A review of a single on premise SQL database, supporting the application, will be undertaken to ensure both that the database itself has been hardened and to provide assurance around the storage of data inside the database. Typical items that are checked within this phase relate to whether the table contents are encrypted (where appropriate), sufficient auditing has been enabled and that the service itself has undergone security hardening such as the removal of default accounts and strong authentication mechanisms being deployed for example. This phase of the assessment will also include a build review of the underlying server build for the database server.

This review will provide

assurance that the configuration of the server is in line with expectations e.g. that Group Policy (if the

server is joined to a domain) has undergone a sufficient level of hardening and that the software installed on the server is up to date and configured securely for example.

Prerequisites: In order to complete this phase of the assessment, the following will be required:

- Credentials to access the server at an administrative level i.e. local admin rights.
- Credentials to access the database at an administrative level i.e. DBA role
- Network connection to RDP onto the server
- IP address and hostname of the target server

1 day at NCC Group Offices - Reporting

A full and detailed report will be authored for the ITHC, in accordance with CHECK guidelines. This report will feature:

- An executive summary, to be used by the senior leadership team to gain a qualitative understanding of the threat landscape of the environment. There is also a table where the number of risks in each identified element are provided, broken out by severity.
- A detailed findings section, which provides understandable write-ups for each issue identified and any affected components, providing comments on the risks and severity.
- Targeted and actionable remediation guidance for each individual issue identified.
- A full list of methodologies that were worked through during the ITHC.

In addition to the report, an issue matrix will be provided which is in spread sheet form. This issue matrix contains each issue identified, along with the risk rating, description and targeted remediation advice. It also has tracking functionality which allows the remediation teams to use it as a working document to improve the security posture of the environment. During the assessment, regular wash-up meetings will be held where progress and the observed issues will be commented upon. This will allow CQC to comment on issues and potentially assist with diagnosis as necessary.

Timescales

This assessment totals 4 days and can be scheduled in within the next 2 weeks. A draft issue matrix, in Microsoft Excel format, and report, in PDF format, will be delivered securely to CQC at the end of the last reporting day for the assessment. The report will also be submitted into the NCC Group QA process for review, after which a final report and spreadsheet will be delivered securely to CQC. The QA process can take 5 working days.

Testing Logistics

It is expected that the web application testing will be conducted remotely from NCC Groups secure testing labs, with the database review being conducted on site at CQC unless remote access can be provided. The assessment will be conducted by 1 CHECK Team Leader, who is also a CREST Applications Certified Consultant.

YOUR RESPONSE

NCC Group Response to Requirement Statement 4

As a pure play cyber security, risk and privacy specialist, working with public and private sector organisations on their cyber security strategies is our "bread and butter". This includes developing testing strategies to provide strong assurance to all organisations we work with. We also have the largest CHECK Certified Testing team with nearly 100 consultants at the respected CHECK Team Leader and CHECK Team Member levels. Our CHECK team delivers on average 40,000 test days a year to over 300 public sector organisations. The skillset of the CHECK team allows for bespoke ITHCs to be completed in a greater level of depth whilst also ensuring that the public sector organisations are worked with in a collaborative fashion to aid improving the security posture of the environment. NCC Group do not believe in conducting compliance style assessments where limited assurance is given to clients which is neither reflective of the security posture of the environment or helpful in terms of improving the security of the environment. Our breadth and depth of experience in this domain is demonstrated by the work we have undertaken and the communities of practice within our business.

We have proven experience of working with HMG and a clear understanding of HMG policy and the enterprise network security architecture. NCC Group operates within a number of NCSC and CREST schemes which require that the mandatory requirements for handling protectively marked data and a clear knowledge of the SPF. As a FTSE 250 listed company we are also fully compliant with all relevant laws and information security standards. An example of a recent engagement that will demonstrate our capability, agility and technical competence in cyber security can be seen below.

3yr Programme of CHECK Testing for Large Central Government Organisation

Goals: To provide CHECK testing to over 12 different programs within the organisation – 36 Month Programme – [REDACTED]

Services Delivered:

- Bespoke Scoping consultancy and recommended testing activities
- Full Official CHECK testing at SC and DV clearance level
- Full Report Debrief
- Post Testing Remediation support

In terms of responsiveness, our clients have longstanding agreements with us as we not only delivery quality consulting but can do so at speed in line with their requirements. We pride ourselves in putting the client first and adapting to your timescales. Our scoping process ensures a quick turnaround without risking technical quality, as we have dedicated technical support functions in NCC Group as well as the majority of the UKs CHECK staff so can understand even the most complex environment and define a scope which delivers the right level of assurance independently. It is not unusual for a client request to be shared in the morning and have a formal scope proposed out the following morning (depending on complexity and availability of CQC in the event there are questions).

Our timescales for delivery are also market leading. Once proposed, the team can be delivering the assessment within a matter of days dependent upon the requirement. Average deployment for larger ITHCs is circa 2 weeks, dependent upon complexity.

PART 3: YOUR PRICES

Once you have completed 'Your Offer' (this document) please refer to the 'Your Prices' template for guidance on how to submit your pricing and discounts for delivering the Buyer's Needs.

As specified in 'The Buyer Needs' this section will count for 20% of your overall evaluation score.

Only if you meet the minimum pass marks of a 2 in all of the evaluation criteria in the previous parts of 'Your Offer' will your prices be evaluated.

Price will be assessed by the maximum points of 20% being awarded to the lowest price as per the calculation below. The Price evaluation will be taken from the cell I30 in Your prices and is the Discounted Estimated Total Cost.

Score =

Discounted estimated total cost* x 20% (maximum mark available)

Tender Price

* Discounted estimated total cost is Cell I30 in 'Your Prices'.

CQC will award the Contract to the Supplier submitting the most economically advantageous tender (i.e. the Tender that achieves the highest combined final score (out of 100%), made up from Your Offer score (maximum score = 80) and Your Prices (maximum score = 20). In the event that two or more Suppliers obtain the same highest combined final score, the Supplier with the highest score for the 'Financial' element will be deemed the winner and awarded the Contract.

Please note it is a mandatory requirement to submit your rate card for information for any future requirements throughout the contract. This will not be used for scoring.

As specified in 'The Buyer Needs' this section will count for 20% of your overall evaluation score.

Failure to complete the pricing schedule in full may result in the tender being rejected. In the event you are unclear with regards to any section, please do not hesitate to contact Care Quality Commission via the Bravo eSourcing portal.

Your Prices

RM3764ii Cyber Security

Please note if you are bidding to supply services under Lot 2, You MUST provide a CHECK Token
Lot 1/1/1

An SSI is bidding to supply services under Lot 4 MUST declare that they have valid CHECK Status.

Your Details	
Supplier Name:	NCC Group Security Services Limited
Project bidding for:	Hypothetical Test Case found in Your Offer option 1A
An application has been built and is hosted on a cloud based PaaS / IaaS. The application build has utilised a number of open source software libraries and will interface over secured internet communications with an internal (on premise) active directory and sql database. Once operational the system will provide services to and gather information from a larger number (C 50,000) of external users via secured web interfaces available on the company website and may also interface with a cloud based DAM system. Please detail the roles and prices you would charge for this requirement.	

Discounts you are willing to apply for this mini competition	
Suppliers cumulative commitment	Discount Percentage
20 Working Days and over, but less than 60	0%
60 Working Days and over, but less than 90	0%
Working Days	
Anything over 90 Working Days	0%

Lot bidding for (Description to be bid)	Roles providing (List of roles to be bid)	Day rate*	T&S	Total	No. Of people	No. of Days	Total cost

Your Prices

RM3764ii Cyber Security Services CSS01-Care Quality Commission PSO 197 Penetration Testing

BUYER'S INTERNAL TRAVEL AND SUBSISTENCE POLICY

The Parties agree that they shall bear their own respective costs and expenses incurred in respect of compliance with their obligations.

This will be discussed at the kick off meeting when the scope of the testing is confirmed.

Where possible CQC are seeking resources that are local to the area in which the work will be undertaken and where expense will not be incurred.

Where this is not possible, any travel and subsistence expenses will need to comply with the CQC Travel and expenses policy

SCHEDULE 2 - HIGH LEVEL DELIVERY PLAN

Please refer to Schedule 1

SCHEDULE 3 - BUYER RESPONSIBILITIES

The Buyer agrees to:

- obtain consent from its ISP and any third party suppliers of the System for the Security Testing to be carried out and, when requested by the Supplier, to provide written evidence of such consent and to notify relevant employees that the Security Testing has been scheduled and that the employees may be monitored; "System" being defined as the systems and networks which the Buyer requires to be security tested or security monitored and/or scanned as part of the Services, together with any software, systems, networks, premises, equipment, data structures, protocols, computers, hardware and firmware linked to the same and data passing across or contained in any of the foregoing;
- that it shall properly and fully back-up all data and copies of all computer programs and data which are held immediately prior to commencement of the Security Testing, and which may be affected by the provision of the Security Testing and, where appropriate, regularly perform backups during the performance of the Security Testing, to enable straightforward recovery and/or reinstatement of any and all data and/or computer programs lost or damaged (whether in whole or part) through provision of the Security Testing; or
- that the Supplier allocates consultants weeks or months in advance and would suffer a loss should the Services or any Service Portion be postponed or cancelled at short notice. As such, the Buyer agrees that it shall pay to the Supplier (as genuinely pre-estimated liquidated damages) an amount to reflect the losses which the Supplier will incur if such cancellation or rescheduling is requested within a set number of days of the start date (the "Cancellation Fee").

The relevant percentages and time periods as referred to above are as follows:

- 1.1.1 cancellation request 8-21 days before the start date: 50% of the scheduled days cost;
- 1.1.2 rescheduling request 8-14 days before the start date with firm re-booking date: 50% of the scheduled days cost; and
- 1.1.3 cancellation or rescheduling request within 7 days of the start date: 100% of the scheduled days cost.

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:	23/12/2019
SoW Reference:	
Buyer:	Care Quality Commission
Supplier:	NCC Group Security Services Limited
Sub-Contractors: (list all sub-contractors)	n/a
Overall Estimated Service Completion Date: (the "Completion Date")	22/12/2021
Duration of SoW (How long the SoW will last – expressed as Working Days)	2 years
Charging Mechanism(s) for this SoW: (Capped/ Time and Materials/ Time and Materials/ Fixed Price/ Milestone deliverables)	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:

Name	Role	Details
TBC	TBC	TBC

Deliverables:

A full and detailed report will be authored for each assessment, in accordance with CHECK guidelines. This report will feature:

- ☐ An executive summary, which can be used by the senior leadership team to gain a qualitative understanding of the threat landscape of the environment. There is also a quantitative element where the number of risks in each identified element are provided, broken down by severity.
- ☐ A detailed findings section, which provides understandable write-ups for each issue identified and any affected components, providing comments on the risks and individual severity ratings.
- ☐ Targeted and actionable remediation guidance for each individual issue identified.
- ☐ A full list of methodologies that were worked through during the assessment.

Additional Requirements

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). Below and published separately.

Contract Charges:

The Maximum Price for this SoW is: [REDACTED]

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.

- 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.

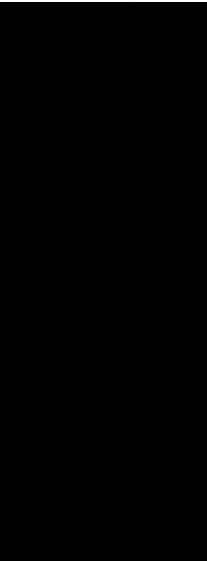
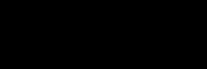
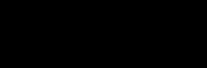
[illegible]

Comments:

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
£761,400	<p>A value of [REDACTED] for CHECK penetration testing services will be provided by NCC Group to Care Quality Commission. The rate card which applies to this draw down value will be:</p> <ul style="list-style-type: none"> • [REDACTED] • [REDACTED] <p>The value was derived from [REDACTED] days, half of the estimated number of required days in CQC's original RFP at the higher rate.</p> <p>Caveats</p> <ul style="list-style-type: none"> • The £761,400 is a committed Value and any remaining value at the end of two years will be invoiced in full. • An example engagement: <ul style="list-style-type: none"> ◦ 3 days on site infrastructure [REDACTED] 		2 years

Fixed Charge	Description	Service Period (or if Payment linked to Milestones then, Milestone Date)	Breakdown By Role and Duration
	<ul style="list-style-type: none">    		
	<ul style="list-style-type: none"> CQC agrees reasonable expenses will be included for NCC resources working at CQC or other third party site and will be detailed in each Invoice 		

Milestone Deliverables


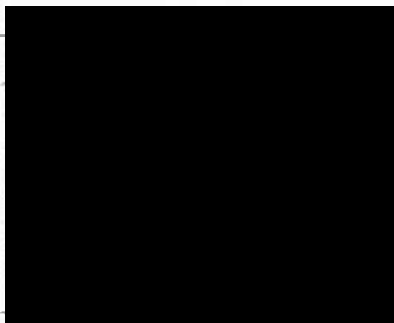
- Milestone Deliverable pricing shall be against the service delivery plan agreed by the Buyer and Supplier at the start of the SoW.
- The Supplier must complete the service Deliverable by the due date.
- The Buyer will review the Deliverable against the agreed acceptance criteria to sign off acceptance
- 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:
Name:		
Title:		
Signature:		

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

SCHEDULE 5 – EXIT PLAN

[Please complete for each SoW in accordance with clause 11] – Not Used

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:

X

X

Select date

Select Date

SCHEDULE 7- BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

NCC Group Business Continuity and Disaster Recovery Plan

NCC Group is exposed to a potential risk that critical business functions or services are impacted following a disruptive incident. A primary business objective is to mitigate the impact of an incident that renders an NCC Group location inaccessible or a critical service unavailable, and to maintain an acceptable level of service to our customers. To achieve this, appropriate arrangements need to be made for business continuity. Our strategy for continuing business in the event of an incident is:

1. to ensure the safety and security of all employees, and
2. to ensure continuity of critical business operations during a disruptive event. The focus of business continuity is primarily to continue business operations at acceptable levels following an incident.

All managers and department heads within NCC Group are responsible for business continuity for their area and are required to have documented plans or know they are part of a larger site plan, which they have approved. They must identify a plan coordinator to assist in the implementation and maintenance of their plans, and provide readiness reporting for their area.

Sound business continuity management principles must be applied when formulating business continuity strategy and plans. Strategy and plans must consider all aspects of the delivery of products and services to customers, including:

- Locations must have an Incident Management Plan (IMP) and Local Incident Management Team (LIMT)
- The potential impact of a worst case scenario incident must be identified in business or customer terms
- Resources required to continue critical functions and services must be defined
- Recovery Time Objectives (RTO) must be defined for critical functions and services, and priorities must be assigned to the continuity of those critical functions and services
- Strategy and plans must provide for the business to meet defined RTOs
- As far as reasonable, there should be geographic diversity between primary and backup sites. To be fully resilient, backup sites should not rely on the same resources as primary sites
- Employees must be aware of their roles and responsibilities in the event of an incident
- Incident Management plans require on-going maintenance and must be updated and tested within the agreed tier structure, or whenever there are material changes, to verify that they are effective and ready at any time
- Business continuity and disaster recovery must be considered in all new product development

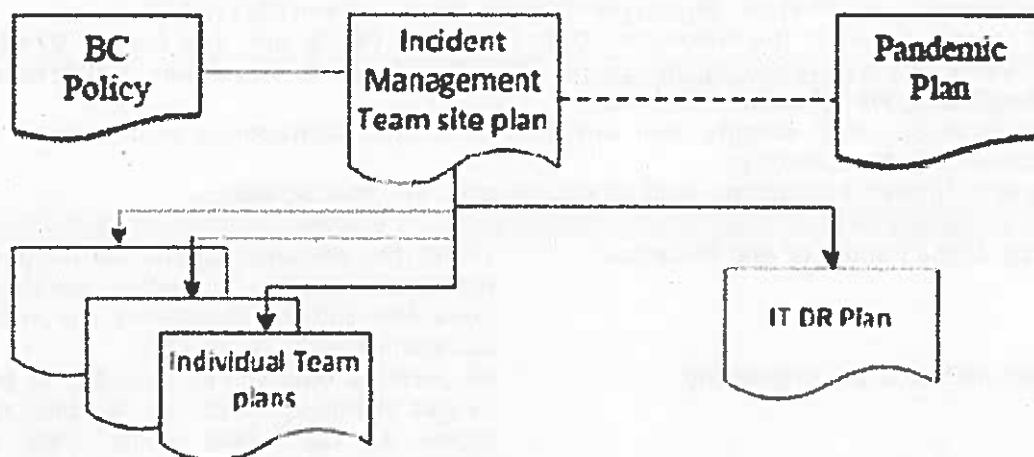
The mission of the Business Continuity Management is to:

- Promote, coordinate, develop and implement preparedness, response, and recovery capabilities within NCC Group
- Maximise resources to facilitate an efficient and effective integrated system
- addressing human services, infrastructure, information technologies, community and economic issues
- Promote awareness of potential disasters, minimize impact of resulting incidents, and assist in the development of proper response methods in worst case
- scenarios based on industry standards, methods, procedures and best practice

KEY SUCCESS FACTORS

- Senior Management buy-in and resource commitment to this mission critical objective
- Heads of department to drive program at the business level
- Approved and implemented policies, procedures, guidelines and standards
- Continued assessment of plan efficiency, gaps and state of readiness
- Continuous improvement through on-going testing and exercising of plans to ensure their viability.

Executive Summary of Business Continuity (BC) plans:



Tier One sites – These plans are invoked by the LIMT when the following criteria have been met

- Communications failure across all sites for more than three or more hours
- Two or more systems and/or sites are down concurrently for three or more hours
- Any problem at any system or network facility that would cause either of the above conditions to be present or there is certain indication that either of the conditions are about to occur.
- Critical Pandemic

Tier Two sites – These plans can be invoked locally or through the invocation of a larger incident

Risk management seeks to manage risk around key products and services delivered by NCC Group. BCM is complimentary to the risk assessment and outlines the risks to operations and services and the consequences. BCM provides a realistic view of how NCC Group will manage those risks in the event of disruption to these services and operations. Maintaining BC Plans enables NCC Group to manage these risks and minimise impact.

All plans are tested over a 2 year cycle:

- Tier one site – will be tested on an annual basis using desk top exercises
- Tier two sites – will conduct a table top exercise biennially and all documentation will be reviewed annually
- Tier three site – due to their size and minimal personnel these sites will not be tested as part of the schedule

SCHEDULE 8 - PROCESSING, PERSONAL DATA AND DATA SUBJECTS

1. The contact details of the Controller's Data Protection Officer are: [REDACTED]
Quality Commission, 3rd Floor, Buckingham Palace Road, London SW1W 9SZ.
2. The contact details of the Processor's Data Protection Officer are: [REDACTED]
[REDACTED] XYZ Building, 2 Hardman Boulevard, Spinningfields, Manchester, M3 3AQ
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 Schedule.

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor in accordance with Clause 13.1.
Subject matter of the processing	No personal data will be accessed or processed as part of this contract. The supplier may have access to CQC data whilst they test our infrastructure and applications but do not have a requirement to process any data.
Duration of the processing	The contract includes a provision for multiple tests (engagements) over the coming 2 years. Each test will last between 2 and 10 days but will not process any CQC data.
Nature and purposes of the processing	As above.
Type of personal data	The supplier will be given temporary CQC IT accounts in order to carry out the necessary tests. Theoretically, they could access any and all CQC data but will, in practice, not access any personal information. The contract with the supplier underlines this with NDA and Confidentiality clauses included.
Categories of Data Subject	In practice none but potentially all categories of data which CQC itself holds and processes.
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	Not applicable.

SCHEDULE 9 – SECURITY REQUIREMENTS

INTERPRETATION AND DEFINITION

For purposes of this Schedule 9, references to Authority shall mean "the Buyer" and references to the Contractor shall mean "the Supplier"

For the purposes of this Schedule 9, unless the context otherwise requires the following provisions shall have the meanings given to them below:

"Authority System" means the Authority's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Authority or the Contractor in connection with the Contract which is owned by or licensed to the Authority by a third party and which interfaces with the Contractor System or which is necessary for the Authority to receive the Services;

"Breach of Security" means the occurrence of unauthorised access to or use of the Premises, the Premises, the Services, the Contractor System, or any ICT or data (including Authority Data) used by the Authority or the Contractor in connection with the Contract.

"Contractor Equipment" means the hardware, computer and telecoms devices and equipment supplied by the Contractor or its Sub-Contractor (but not hired, leased or loaned from the Authority) for the provision of the Services;

"Contractor Software" means software which is proprietary to the Contractor, including software which is or will be used by the Contractor for the purposes of providing the Services and which is specified as such in Schedule 8.

"Contractor System" means the information and communications technology system used by the Contractor in performing the Services including the Software, the Contractor Equipment and related cabling (but excluding the Authority System);

"ICT" means Information Communications Technology and includes a diverse set of technological tools and resources used to communicate, and to create, disseminate, store and manage information, including computers, the Internet, broadcasting technologies (radio and television), and telephony.

"Protectively Marked" shall have the meaning as set out in HMG Security Policy Framework.

"Security Plan" means the Contractor's security plan prepared pursuant to paragraph 3 an outline of which is set out in an Appendix to this Schedule 8.

"Software" means Specially Written Software, Contractor Software and Third Party Software.

"Specially Written Software" means any software created by the Contractor (or by a third party on behalf of the Contractor) specifically for the purposes of this Contract.

"Third Party Software" means software which is proprietary to any third party which is or will be used by the Contractor for the purposes of providing the Services including the software and which is specified as such in Schedule 7.

1. INTRODUCTION

This Schedule 9 covers:

- 1.1 principles of security for the Contractor System, derived from HMG Security Policy Framework, including without limitation principles of physical and information security;
- 1.2 wider aspects of security relating to the Services;
- 1.3 the creation of the Security Plan;
- 1.4 audit and testing of the Security Plan; and
- 1.5 breaches of security.

2. PRINCIPLES OF SECURITY

- 2.1 The Contractor acknowledges that the Authority places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Premises and the security for the Contractor System. The Contractor also acknowledges the confidentiality of Authority Data.
- 2.2 The Contractor shall be responsible for the security of the Contractor System and shall at all times provide a level of security which:
 - 2.2.1 is in accordance with Good Industry Practice and Law;
 - 2.2.2 complies with HMG Security Policy Framework; and
 - 2.2.3 meets any specific security threats to the Contractor System.
- 2.3 Without limiting paragraph 2.2, the Contractor shall at all times ensure that the level of security employed in the provision of the Services is appropriate to maintain the following at acceptable risk levels (to be defined by the Authority):
 - 2.3.1 loss of integrity of Authority Data;
 - 2.3.2 loss of confidentiality of Authority Data;

- 2.3.3 unauthorised access to, use of, or interference with Authority Data by any person or organisation;
- 2.3.4 unauthorised access to network elements, buildings, the Premises, and tools used by the Contractor in the provision of the Services;
- 2.3.5 use of the Contractor System or Services by any third party in order to gain unauthorised access to any computer resource or Authority Data; and
- 2.3.6 loss of availability of Authority Data due to any failure or compromise of the Services.
- 2.3.7 processing and storage of authority data within the UK or by exception within the EEA. Any processing outside of the UK must be subject to specific approval by the Authority.

3. SECURITY PLAN

- 3.1 The Contractor shall develop, implement and maintain a Security Plan to apply during the Contract Period (and after the end of the term as applicable) which will be approved by the Authority, tested, periodically updated and audited in accordance with this Schedule 9.
- 3.2 A draft Security Plan provided by the Contractor as part of its bid is set out herein.
- 3.3 Prior to the Commencement Date the Contractor will deliver to the Authority for approval the final Security Plan which will be based on the draft Security Plan set out herein.
- 3.4 If the Security Plan is approved by the Authority it will be adopted immediately. If the Security Plan is not approved by the Authority the Contractor shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit to the Authority for approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Security Plan following its resubmission, the matter will be resolved in accordance with clause 19 (Dispute Resolution). No approval to be given by the Authority pursuant to this paragraph 3.4 may be unreasonably withheld or delayed. However any failure to approve the Security Plan on the grounds that it does not comply with the requirements set out in paragraphs 3.1 to 3.4 shall be deemed to be reasonable.
- 3.5 The Security Plan will set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the

Services and all processes associated with the delivery of the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with:

- 3.5.1 the provisions of this Schedule 9;
 - 3.5.2 the provisions of Schedule 1 relating to security;
 - 3.5.3 the Information Assurance Standards;
 - 3.5.4 the data protection compliance guidance produced by the Authority;
 - 3.5.5 the minimum set of security measures and standards required where the system will be handling Protectively Marked or sensitive information, as determined by the Security Policy Framework;
 - 3.5.6 any other extant national information security requirements and guidance, as provided by the Authority's IT security officers; and
 - 3.5.7 appropriate ICT standards for technical countermeasures which are included in the Contractor System.
- 3.6 The references to Quality Standards, guidance and policies set out in this Schedule shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such Quality Standards, guidance and policies, from time to time.
- 3.7 If there is any inconsistency in the provisions of the above standards, guidance and policies, the Contractor should notify the Authorised Representative of such inconsistency immediately upon becoming aware of the same, and the Authorised Representative shall, as soon as practicable, advise the Contractor which provision the Contractor shall be required to comply with.
- 3.8 The Security Plan will be structured in accordance with ISO/IEC27002 and ISO/IEC27001 or other equivalent policy or procedure, cross-referencing if necessary to other schedules of the Contract which cover specific areas included within that standard.
- 3.9 The Security Plan shall not reference any other documents which are not either in the possession of the Authority or otherwise specified in this Schedule 9.

4. AMENDMENT AND REVISION

- 4.1 The Security Plan will be fully reviewed and updated by the Contractor annually or from time to time to reflect:
- 4.1.1 emerging changes in Good Industry Practice;
 - 4.1.2 any change or proposed change to the Contractor System, the Services and/or associated processes;
 - 4.1.3 any new perceived or changed threats to the Contractor System;
 - 4.1.4 changes to security policies introduced Government-wide or by the Authority; and/or
 - 4.1.5 a reasonable request by the Authority.
- 4.2 The Contractor will provide the Authority with the results of such reviews as soon as reasonably practicable after their completion and amend the Security Plan at no additional cost to the Authority.
- 4.3 Any change or amendment which the Contractor proposes to make to the Security Plan (as a result of an Authority request or change to Schedule 1 or otherwise) shall be subject to a Variation and shall not be implemented until Approved.

5. AUDIT, TESTING AND PROTECTIVE MONITORING

- 5.1 Not Used
- 5.2 NOT USED.
- 5.3 Where any Security Test carried out pursuant to paragraphs 5.1 or 5.2 reveals any actual or potential security failure or weaknesses, the Contractor shall promptly notify the Authority of any changes to the Security Plan (and the implementation thereof) which the Contractor proposes to make in order to correct such failure or weakness. Subject to Approval in accordance with paragraph 4.3, the Contractor shall implement such changes to the Security Plan in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the Security Plan to address a non-compliance with HMG Security Policy Framework or security requirements, the change to the Security Plan shall be at no additional cost to the Authority. For the purposes of this paragraph, a weakness means a vulnerability in security and a potential security failure means a possible breach of the Security Plan or security requirements.

6. BREACH OF SECURITY

- 6.1 Either Party shall notify the other immediately upon becoming aware of any Breach of Security including, but not limited to an actual, potential or attempted breach, or threat to, the Security Plan.
- 6.2 Upon becoming aware of any of the circumstances referred to in paragraph 6.1, the Contractor shall immediately take all reasonable steps necessary to:
- 6.2.1 remedy such breach or protect the Contractor System against any such potential or attempted breach or threat; and
 - 6.2.2 prevent an equivalent breach in the future;
 - 6.2.3 collect, preserve and protect all available audit data relating to the incident and make it available on request to the Authority;
 - 6.2.4 investigate the incident and produce a detailed report for the Authority within 5 working days of the discovery of the incident.
- 6.3 Such steps shall include any action or changes reasonably required by the Authority. If such action is taken in response to a breach that is determined by the Authority acting reasonably not to be covered by the obligations of the Contractor under the Contract, then the Contractor shall be entitled to refer the matter to the variation procedure set out in the Contract.
- 6.4 The Contractor shall as soon as reasonably practicable provide to the Authority full details (using such reporting mechanism as may be specified by the Authority from time to time) of such actual, potential or attempted breach and of the steps taken in respect thereof.

7. CONTRACT EXIT – SECURITY REQUIREMENTS

In accordance with clause H7 of the Contract, on termination of the Contract, either via early termination or completion of the Contract then the Contractor will either return all data to the Authority or provide a certificate of secure destruction using an industry and Authority approved method. Destruction or return of the data will be specified by the Authority at the time of termination of the Contract.

APPENDIX 1- OUTLINE SECURITY PLAN

ANNEX 1: BASELINE SECURITY REQUIREMENTS

1. SECURITY CLASSIFICATION OF INFORMATION

- 1.1 If the provision of the Services requires the Contractor to Process Authority Data which is classified as OFFICIAL, OFFICIAL-SENSITIVE or Personal Data, the Contractor shall implement such additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable legislative and regulatory obligations.

2. END USER DEVICES

- 2.1 The Contractor shall ensure that any Authority which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Authority except where the Authority has given its prior written consent to an alternative arrangement.
- 2.2 The Contractor shall ensure that any device which is used to Process Authority Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/end-user-device-security>.

2A. TESTING

The Contractor shall at their own cost and expense, procure a CHECK or CREST Certified Contractor to perform an ITHC or Penetration Test prior to any live Authority data being transferred into their systems. The ITHC scope must be agreed with the Authority to ensure it covers all the relevant parts of the system that processes, stores or hosts Authority data.

3. DATA PROCESSING, STORAGE, MANAGEMENT AND DESTRUCTION

- 3.1 The Contractor and Authority recognise the need for the Authority's Information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Contractor must be able to state to the Authority the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Authority Data will be subject to at all times.
- 3.2 The Contractor shall not, and shall procure that none of its Sub-contractors, process Authority Data outside the EEA without the prior written consent of the Authority and the Contractor shall not change where it or any of its Sub-contractors process Authority Data without the Authority's prior written consent which may be subject to conditions.
- 3.3 The Contractor must be able to demonstrate they can supply a copy of all data on request or at termination of the service, and must be able to securely erase or destroy all data and media that the Authority data has been stored and processed on.

The Contractor shall:

- 3.3.1 provide the Authority with all Authority Data on demand in an agreed open format;

3.3.2 have documented processes to guarantee availability of Authority Data in the event of the Contractor ceasing to trade;

3.3.3 securely destroy all media that has held Authority Data at the end of life of that media in line with Good Industry Practice; and

3.3.4 securely erase any or all Authority Data held by the Contractor when requested to do so by the Authority.

4. NETWORKING

4.1 The Authority requires that any Authority Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted when transmitted.

4.2 The Authority requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. SECURITY ARCHITECTURES

5.1 Contractors should design the service in accordance with:

- NCSC " Security Design Principles for Digital Services "
- NCSC " Bulk Data Principles "
- NSCS " Cloud Security Principles "

6. PERSONNEL SECURITY

6.1 All Contractor Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard or equivalent including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record. The Contractor maybe required implementing additional security vetting for some roles.

7. IDENTITY, AUTHENTICATION AND ACCESS CONTROL

7.1 The Contractor must operate an appropriate access control regime to ensure that users and administrators of the service are uniquely identified. The Contractor must retain records of access to the physical sites and to the service.

8. AUDIT AND PROTECTIVE MONITORING

8.1 The Contractor shall collect audit records which relate to security events in delivery of the service or that would support the analysis of potential and

actual compromises. In order to facilitate effective monitoring and forensic readiness such Contractor audit records should (as a minimum) include:

8.1.1 regular reports and alerts setting out details of access by users of the service, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data. The retention periods for audit records and event logs must be agreed with the Authority and documented.

8.2 The Contractor and the Authority shall work together to establish any Anadditional audit and monitoring requirements for the ICT Environment.

8.3 The Contractor shall retain audit records collected in compliance with this Paragraph 8.3 for a period of at least 6 months.

9. VULNERABILITIES AND CORRECTIVE ACTION

9.1 Contractors shall procure and implement security patches to vulnerabilities in accordance with the timescales specified in the NCSC Cloud Security Principle 5.

9.2 Contractor must ensure that all COTS Software and Third Party COTS Software be kept up to date such that all Contractor COTS Software and Third Party COTS Software are always in mainstream support.

10. RISK ASSESSMENT

10.1 The Contractor should perform a technical information risk assessment on the service supplied and be able to demonstrate what controls are in place to address those risks.

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>