Crown Commercial Service

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

Order Form

This Order Form is issued in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100 dated 16/06/2020 between the Supplier (as defined below) and the Minister for the Cabinet Office (the "**Framework Agreement**") and should be used by Buyers after making a direct award or conducting a further competition under the Framework Agreement.

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

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

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

This Order Form shall comprise:

1. This document headed "Order Form";
2. Attachment 1 – Services Specification, inclusive of Clarification Question Log;
3. Attachment 2 – Charges and Invoicing;
4. Attachment 3 – Implementation Plan;
5. Attachment 4 – Service Levels and Service Credits;
6. Attachment 5 – Key Supplier Personnel and Key Sub-Contractors;
7. Attachment 6 – Software;
8. Attachment 7 – Financial Distress;
9. Attachment 8 - Governance
10. Attachment 9 – Schedule of Processing, Personal Data and Data Subjects;
11. Attachment 10 – Transparency Reports;
12. Attachment 11 – Fujitsu Submission to Questions 3.2.1 to 3.2.7 and 3.3.1; and
13. Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses.

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

the Framework, except Framework Schedule 18 (Tender);

the Order Form;

Crown Commercial Service

the Call Off Terms; and

Framework Schedule 18 (Tender).

Section A
General information

Contract Details	
Contract Reference:	SR788241953
Contract Title:	EDR and Vulnerability Managed Service
Contract Description:	Provision of a 2-year managed service to support Endpoint Detection Response and Vulnerability
Contract Anticipated Potential Value: this should set out the total potential value of the Contract	£280,000 plus VAT
Estimated Year 1 Charges:	£140,000 plus VAT
Commencement Date: this should be the date of the last signature on Section E of this Order Form	22/09/2022
Service Commencement Date:	Tenable: 1st October 2022 Crowdstrike: 17th October 2022

Buyer details
Buyer organisation name Her Majesty's Revenue & Customs
Billing address Your organisation's billing address - please ensure you include a postcode 100 Parliament Street, London, SW1A 2BQ
Buyer representative name The name of your point of contact for this Order *REDACTED*
Buyer representative contact details Email and telephone contact details for the Buyer's representative. This must include an email for the purpose of Clause 50.6 of the Contract. *REDACTED*

Crown Commercial Service

Buyer Project Reference
Please provide the customer project reference number.
SR788241953

Supplier details

Supplier name
The supplier organisation name, as it appears in the Framework Agreement
Fujitsu Services Limited

Supplier address
Supplier's registered address
Lovelace Road, Bracknell, RG12 8SN, United Kingdom

Supplier representative name
The name of the Supplier point of contact for this Order
REDACTED

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

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

EDR and Vulnerability Managed Service

Guarantor details

Guidance Note: Where the additional clause in respect of the guarantee has been selected to apply to this Contract under Part C of this Order Form, include details of the Guarantor immediately below.

Guarantor Company Name
The guarantor organisation name
Not Applicable

Guarantor Company Number
Guarantor's registered company number
Not Applicable

Guarantor Registered Address
Guarantor's registered address
Not Applicable

Crown Commercial Service

Section B
Part A – Framework Lot

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

1.	TECHNOLOGY STRATEGY & SERVICES DESIGN	☐
2.	TRANSITION & TRANSFORMATION	☐
3.	OPERATIONAL SERVICES	
	a: End User Services	☐
	b: Operational Management	✓
	c: Technical Management	☐
	d: Application and Data Management	☐
5.	SERVICE INTEGRATION AND MANAGEMENT	☐

Part B – The Services Requirement

Commencement Date
See above in Section A

Contract Period

2 Years

Initial Term Months
24 Months

Extension Period (Optional) Months
12 Months

Minimum Notice Period for exercise of Termination Without Cause 30 Calendar Days

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

The Supplier shall provide the Services from the following Sites:
Buyer Premises:

Crown Commercial Service

Given the current restrictions due to COVID-19, the Supplier will need to work virtually to begin with. The specifics of how this will be handled will be discussed with the Supplier upon contract commencement. Once measures have been relaxed the primary locations will be:

HMRC Stratford, London
Benton Park View, Newcastle
Plaza 2, Telford
Trinity Bridge House, Salford
7&8 Wellington Place, Leeds

Supplier Premises:
Not Applicable

Third Party Premises:
Not Applicable

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

HMRC shall provide the following Buyer Software as a Buyer Responsibility:

- Tenable
- Crowdstrike.

The Volume of licenses required for the Services is further set out in Attachment 1

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

Not Applicable

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

Please refer to
https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework

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

Not Applicable

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

Crown Commercial Service

Third Party Public Liability Insurance (£) - Not less than one million pounds (£1,000,000) in respect of any one occurrence, the number of occurrences being unlimited, but one million pounds (£1,000,000) any one occurrence and in the aggregate per annum in respect of products and pollution liability.

Professional Indemnity Insurance (£) - Not less than one million pounds (£1,000,000) in respect of any one claim and in the aggregate per annum

Buyer Responsibilities
Guidance Note: list any applicable Buyer Responsibilities below.

Not Applicable

Goods
Guidance Note: list any Goods and their prices.

Not Applicable

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

Governance Schedule	Tick as applicable
Part A – Short Form Governance Schedule	✓
Part B – Long Form Governance Schedule	☐

The Part selected above shall apply this Contract.

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

Change Control Schedule	Tick as applicable
Part A – Short Form Change Control Schedule	✓
Part B – Long Form Change Control Schedule	☐

Crown Commercial Service

Section C

Part A - Additional and Alternative Buyer Terms

Additional Schedules and Clauses *(see Annex 3 of Framework Schedule 4)*
This Annex can be found on the RM6100 CCS webpage. The document is titled RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5.

Part A – Additional Schedules
Guidance Note: Tick any applicable boxes below

Additional Schedules	Tick as applicable
S1: Implementation Plan	☐
S2: Testing Procedures	☐
S3: Security Requirements (either Part A or Part B)	Part A ☐ or Part B ☐
S4: Staff Transfer	☐
S5: Benchmarking	☐
S6: Business Continuity and Disaster Recovery	☐
S7: Continuous Improvement	☐
S8: Guarantee	☐
S9: MOD Terms	☐
S10: HMRC Authority Mandatory Terms	✓

Part B – Additional Clauses
Guidance Note: Tick any applicable boxes below

Additional Clauses	Tick as applicable
C1: Relevant Convictions	☐
C2: Security Measures	☐
C3: Collaboration Agreement	☐

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

Part C - Alternative Clauses
Guidance Note: Tick any applicable boxes below

The following Alternative Clauses will apply:

Alternative Clauses	Tick as applicable
Scots Law	☐
Northern Ireland Law	☐
Joint Controller Clauses	☐

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

Crown Commercial Service

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

S10: HMRC Authority Mandatory Terms has been included as:

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

Crown Commercial Service

Additional Schedule S3 (Security Requirements)
REDACTED

Crown Commercial Service

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

Not Applicable

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

Not Applicable

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

An executed Collaboration Agreement shall be delivered from the Supplier to the Buyer within the stated number of Working Days from the Commencement Date:

Not Applicable

Section D
Supplier Response

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

Call-Off Contract Attachment 2-Charges and Invoicing
- Part B Service Charges and Onboarding Charges
- Part C-Supplier Personnel Rate Card for Calculation of Time & Materials Charges

Section E
Contract Award

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

Crown Commercial Service

SIGNATURES

For and on behalf of the Supplier

Name	*REDACTED*
Job role/title	*REDACTED*
Signature	*REDACTED*
Date	*REDACTED*

For and on behalf of the Buyer

Name	*REDACTED*
Job role/title	*REDACTED*
Signature	*REDACTED*
Date	*REDACTED*

Crown Commercial Service

Attachment 1 – Services Specification

1. STATEMENT OF REQUIREMENTS

1.1 Background to HMRC

1.1.1 HM Revenue & Customs (HMRC) is the UK's tax, payment, and customs authority. Its ability to collect and distribute funds underpins the delivery of the UK's public services and the targeted support to families and individuals swiftly and accurately. HMRC's services are part of the UK's critical national infrastructure.

1.1.2 HMRC also protects the fairness of the tax system by making it hard for the dishonest minority to avoid payment of their taxes, undertaking debt collection and legal enforcement of those who try to avoid or evade their responsibilities. It has a workforce of approximately 58,700 FTEs, ranging from customer service advisors to data analysts.

1.1.3 For the financial year 2020-21, HMRC:

- Collected £608.8bn in total tax revenues
- £30.4bn additional tax generated through tackling avoidance, evasion, and other non-compliance
- 1.5m businesses using Making Tax Digital for VAT since launch
- 3000+ businesses supported to prepare for the end of UK's transition from the EU
- 11.5m jobs supported through the Coronavirus Job Retention Scheme up to 31 March 2021
- 2.7m people supported by the Self-Employment Income Support Scheme up to 31 March 2021

1.1.4 HMRC has five strategic objectives that guide everything it does:

- Collect the right tax and pay out the right financial support
- Make it easy to get tax right and hard to bend or break the rules
- Maintain taxpayers' consent through fair treatment and protect society from harm
- Make HMRC a great place to work
- Support wider government economic aims through a resilient, agile tax administration system

1.1.5 Our vision is to be a trusted, modern tax and customs department, and our work is underpinned by our values:

- We are professional
- We act with integrity
- We show respect
- We are innovative

1.2 Background to the Endpoint Detection & Response (EDR) and Vulnerability Assessment Tooling

There is a risk that HMRC will be subject to significant cyber-attack without the protection of Endpoint Detection Response and Vulnerability Assessment tooling leading to a catastrophic loss of buildings and services and significant data breach.
Cyber security threats are evolving and finding ways to bypass traditional file signature based anti-virus solutions e.g. McAfee anti-virus.
Endpoint Detection and Response (EDR) systems look for indication of malware behaviour rather than simply detecting known malware files.
HMRC have conducted a lengthy procurement and evaluation process to select a server EDR solution and CrowdStrike Falcon was the best fit to requirements (and is the market leader).
The Vulnerability Assessment tool will assess the entire HMRC Server estate for any software that can be exploited and the tooling for Vulnerability Assessment is Tenable.sc

1.3 Background to Requirement

Endpoint Detection and Response (EDR) for Servers Technology works by providing continuous and comprehensive real time visibility into what is happening on the HMRC servers. Behavioural analysis and actionable intelligence is then applied to the servers to identify potential Security Risks/Breaches and Attacks. The CrowdStrike Platform is a SaaS solution provided by CrowdStrike, servicing server endpoints utilising up to 84m compute hours over a 3 year profile. Integration points are noted elsewhere in these requirements. The core IT functions and integrations for the CrowdStrike solution will be in place before this agreement commences. CrowdStrike was launched into deployment in December 2021. HMRC have currently deployed CrowdStrike to 250 servers with the expectation that this will increase to a minimum of 3000 by April 2023. The deployment will continue into 2024 until all servers in scope have been deployed to.

Tenable Security Centre (SC) works by allowing Service Owners to proactively identify vulnerabilities that exist in the different HMRC environments. This information can then be leveraged to reduce the potential of security risks, attacks and other cyber security threats. The Tenable Platform scope is an on-prem and cloud solution initially built by HMRC. The platform will include up to 3 management servers, 3 scanners in LDC, 5 scanners in CH, 2 scanners in cloud and 2 scanners in Sysman, with potential for deployment of additional scanners to accommodate future scanning requirements and coverage. The 2 Sysman scanners are a tactical solution and will be decommissioned later in the year. The maximum Tenable IP licences will be 20,000. Current licence usage is 12,223 and is expected to increase to 15,000 by April 2023.

The service is currently provided by a team of 5 FTE (3 x Engineers, 1 x Senior Engineer and 1 x Service Manager) with the CrowdStrike rollout in its infancy. Coverage will be increased to 5,000 servers by end FY22-23, then 10,000 servers by end FY23-24, and 15,000 by end FY24-25.

A Managed Service is required to ensure that both these systems are maintained, and any alerts or incidents are acted upon.

Crown Commercial Service

1.4 General Requirements

The scope of the Managed Service provider is limited to support services for CrowdStrike Falcon Insight and Tenable.sc and includes;

1. IT Service management (including Problem Management, Incident Management, Change Management, release Management, configuration Management etc.)
2. Knowledge Management
3. Technical Operations Management (this includes patching, relevant upgrades, Integration etc.)
4. Technical Support
5. Support on-boarding & off-boarding of users
6. Upskilling and Training
7. Monitoring and Reporting
8. Platform scope for CrowdStrike is SAAS while Platform scope for Tenable is both on-prem and cloud.
9. Vendor Management
10. Governance

1.5 Core Deliverables

The Supplier will be responsible for providing the following deliverables:

CrowdStrike:

A. The Supplier and Service Level Management

- Managing the relationship with CrowdStrike and Roadmap of Services – the Roadmap is a view of all things to come, a projection of future releases and functionality. Any planned research and development including end of life and its replacement. This can also include cost and industry trends and findings into new cyber security.
- Pro-active engagement with Technical Account Manager (TAM) to resolve any issues around Server Sensor Agent
- Review and measure all Service Level Agreements

B. Maintaining and updating Support Documentation and Knowledge Articles

- This is all the relevant operational support guides and Knowledge - within service central which are references by service desk team to help identify the impact and urgency of any tickets they receive from HRMC stakeholders to form initial diagnosis and trouble shooting and escalate accordingly within the HRMC IT support function.
- Taking ownership and responding to Business Area queries and issues

C. System Availability

- Monitoring of all CrowdStrike products and services consumed by HMRC, including the SaaS Portal and functionality
- Proactive identification of additional resources required for the completion of ongoing Project related activities

D. Integration

- Monitor the Splunk CrowdStrike interface (Alerting), and resolve any issues or anomalies

- Monitor the CrowdStrike Discovery integrations (AWS & Azure environments), and resolve any issues or anomalies

E. Release Management

- Provide support to the installation and maintenance of the CrowdStrike Sensor Agent
- Provide Support with any issues regarding the registration of new AWS or Azure Accounts within CrowdStrike
- Provide Support to the QA and Pilot Testing Function (MDTS)

F. Licensing Management

- Monitoring compute consumption based on CrowdStrike license usage for Cloud
- Monitoring subscription-based license usage on Crown Hosting environment
- Managing the communication to Stakeholders of any potential forecast breach of licensing.

Tenable:

G. The Supplier and Service Level Management

- Managing the relationship with Tenable and Roadmap of Services – the Roadmap is a view of all things to come, a projection of future releases and functionality. This includes any products coming to end of life and their replacement.
- Where appropriate, engagement with the Customer Success Manager and Senior Security Engineer to resolve key issues. In most scenarios, tickets should be raised through the Tenable Community Support Portal.
- Review and measure all Service Level Agreements

H. Maintaining and updating Support Documentation and Knowledge Articles

- This is all the relevant operational support and build guides.
- Knowledge Articles within service central. These are references for the service desk team to help identify the impact and urgency of any tickets they receive from HRMC stakeholders to conduct initial diagnosis and trouble shooting before escalating accordingly within the HRMC IT support function.
- Taking ownership and responding to Business Area queries and issues

I. System Availability

- The monitoring of Tenable products and services consumed by HMRC across Cloud Environments, Crown Hosting and Legacy Environment, including the Core Management Platform and Nessus scanners

J. Integration

- Monitor the Tenable.SC integrations including SIEM, Hashicorp Vault and Azure AD and resolve any issues or anomalies

K. Release Management

- Ensure that only supported versions of agents are running on the estate, upgrading agent versions previously deployed where necessary and ensuring that only supported agent versions are deployed thereafter

L. Licensing Management

- Monitoring the IP licence consumption for Tenable.SC, ensuring it doesn't breach the maximum threshold

- Managing the communication to Stakeholders of any potential forecast breach of licensing

1.6 Specific Outputs

1.6.1 The Supplier will be responsible for providing the following deliverables:

Mandatory Requirements

CrowdStrike:

1	1.1	Crowdstrike	**Security Clearance**	The Supplier will be a trusted vendor with appropriate security clearance. They will not have a view of vulnerabilities on the HMRC Estate. Security Clearance to be through HMRC governance process for UK resource.
2	1.2	Crowdstrike	**Support Hours**	Support Hours for Crowdstrike should align to HMRC 'Standard Service Level Package' - 07:00hrs to 19:00 hrs, Monday to Friday, excluding Bank Holidays
3	1.3	CrowdStrike	**Service Availability**	Service Availability should align to HMRC 'Standard Service Level Package' >= 99.00% For information - the Crowdstrike vendor's Service Availability Level is 99.9%
4	1.4	CrowdStrike	**HMRC Staff Up-Skilling**	HMRC require their team to be up-skilled by the Supplier for the duration of the contract. This will be measured through regular service reviews and evidenced through take on of skills by HMRC staff. For CrowdStrike the up-skilling is with HMRC delivery groups (there are 60+ delivery groups, some with sub-organisations) that may deploy the CrowdStrike agent. Knowledge articles should be maintained/provided to the HMRC delivery groups for this purpose together with on-going advisory role. Upskilling is also with the HMRC cyber security team to advise that team of features and functions that are available for use and to provide access to the CrowdStrike university for up to 70 HMRC staff. Responses to ad-hoc queries about technical features within the tooling set should be provided, with supporting documentation where relevant.
5	1.5	Crowdstrike	**Access to Tooling and Acceptable Use Policy**	Access to the tooling systems under the scope this agreement will be via HMRC workstations and Azure SSO with Conditional Access enabled, identities and network routes provided by HMRC. The Acceptable Use Policy for use of HMRC assets must be complied with at all times. Access to problem management and change management tooling via this method would also be required via HMRC provided guest accounts where possible.

6	1.6	Crowdstrike	**Support Profile**	The profile of the support will be: SOIM Service Operations Service Management, IM Incident Management following HMRC procedures and policies Problem Management including root cause analysis to meet HMRC procedures and policies

Tena-ble: 7	1.7	Tenable	**Security Clearance**	The Supplier will be a trusted vendor with appropriate security clearance. They will not have a view of vulnerabilities on the HMRC Estate. Security Clearance to be through HMRC governance process for UK resource.
8	1.8	Tenable	**Support Hours**	Support Hours for Tenable and Crowdstrike should align to HMRC 'Standard Service Level Package' - 07:00hrs to 19:00 hrs, Monday to Friday, excluding Bank Holidays
9	1.9	Tenable	**Service Availability**	Service Availability should align to HMRC 'Standard Service Level Package' >= 99.00%
10	1.10	Tenable	**HMRC Staff Up-Skilling**	HMRC require their team to be up-skilled by the Supplier for the duration of the contract. This will be measured through regular service reviews and evidenced through take on of skills by HMRC staff. For Tenable there are HMRC delivery group users (approximately 20 user groups) of the Tenable system, for those users a Training Plan should be provided in addition to knowledge articles. The Supplier should also work with the HMRC CSTS team to make best use/configuration of the Tenable solution.
11	1.11	Tenable	**Access to Tooling and Acceptable Use Policy**	Access to the tooling systems under the scope this agreement will be via HMRC workstations and Azure SSO with Conditional Access enabled, identities and network routes provided by HMRC. The Acceptable Use Policy for use of HMRC assets must be complied with at all times. Access to problem management and change management tooling via this method would also be required via HMRC provided guest accounts where possible. Account sign-off for Tenable to be managed by HMRC.
12	1.12	Tenable	**Support Profile**	The profile of the support will be: SOIM Service Operations Service Management, IM Incident Management following HMRC procedures and policies Problem Management including root cause analysis to meet HMRC procedures and policies

Operational Support

CrowdStrike:

1	2.1	CrowdStrike	**Support Scope**	Responsible for monitoring, problem management and incident resolution, knowledge management of the Crowdstrike SaaS platform, integrations to that platform, agents deploy that provide data to that platform. Responsible for the Agent Version Quality Assurance Process and associated assets
2	2.2	CrowdStrike	**Agent Version Quality Assurance Process - Backup & Restore of Process Components**	The objective of the CrowdStrike Agent Version Quality Assurance Process is defined in the Governance section below. Ensure the CrowdStrike Agent Version Quality Assurance Process components (test scripts and test endpoint infrastructure builds) can be restored in the event of an outage or system change that needs to be recovered. Recovery point must be 24 hours. Recovery time must be 24 hours. The quality assurance process will involve up to ten endpoints for testing purposes. Supplier to produce Backup schedules, Backup Windows, Incremental or Full Backup, Snapshots taken beforehand, document all retention periods, roll-back and recovery process, check data integrity of backups, Testing of the Restore Process on a Quarterly basis
3	2.3	CrowdStrike	**Agent Version Quality Assurance Process - Patching of Server Endpoints Used for Testing**	The objective of the CrowdStrike Agent Version Quality Assurance Process is defined in the Governance section below. Ensure virtual machines used in the CrowdStrike Agent Version Quality Assurance Process are correctly patched at OS level to meet HMRC security policies and standards. The CrowdStrike Agent Version Quality Assurance Process may use up to ten test server endpoints.
4	2.4	CrowdStrike	**Service Monitoring**	The monitoring of a continual endpoint detection and response service across Cloud Environment and Crown Hosting Environment. Monitoring includes ensuring the CrowdStrike portal is active, ensuring agents deployed are functioning as expected, ensuring coverage of agents is as expected and licence usage (compute hours model) is compliant and communicated to business owner and IT Asset Management. SYSTEM AVAILABILITY Monitoring of all CrowdStrike products and services consumed by HMRC, including the SaaS Portal and functionality INTEGRATION and OPERATION Monitor the Splunk CrowdStrike interface (Alerting), and resolve any issues or anomalies Monitor the CrowdStrike Discovery integrations (AWS & Azure environments), and resolve any issues or anomalies Monitor the CrowdStrike agent implementation (AWS, Azure and Crown Hosting environments), and resolve any issues or anomalies The response the Supplier should provide in relation to issues/problems found during monitoring or raised by other parties is defined in 'CrowdStrike - Problem Management and

				Reporting of Support Issues'. See Operational support 13 2.1 Crowdstrike Problem Management and Reporting of Support Issues
5	2.5	CrowdStrike	**Agent Versions**	Ensure that only supported versions of agents are running on the estate, upgrading agent versions previously deployed where necessary and ensuring that only supported agent versions are deployed thereafter
6	2.6	CrowdStrike	**Problem Management and Reporting of Support Issues**	The incident resolution and problem management of items that arise in 'CrowdStrike - Service Monitoring' above - including ownership of issues to the point of resolution, liaison and ticket management with the CrowdStrike vendor, liaison and ticket management with HMRC customer delivery groups and supporting IT teams to manage issues to the point of resolution, the reporting of any potential breach of licence usage to the HMRC business owner and IT Asset Management. Note that this explicitly includes the support of CrowdStrike agents that have been deployed to the HMRC server estate. Where resolution of issues has dependency upon other support parties (be they HMRC or third party) the Supplier is to liaise with and manage the activities of those parties to the point of resolution.
7	2.7	CrowdStrike	**Deployment Advice and Feature Guidance**	RELEASE MANAGEMENT Provide advice and guidance to HMRC delivery groups (60+ with some sub-organisations) on deployment options for CrowdStrike agents should the delivery group wish to deploy. Provide responses to frequently asked questions from delivery groups or from other support teams. Provide Support with any issues regarding the registration of new AWS or Azure Accounts within CrowdStrike Review Release Notes and advise Cyber Security Team of any new / roadmap features available Provide advice and guidance to HMRC parties wishing to better understand the features of the CrowdStrike product at technical level
8	2.8	Crowdstrike	**Incident Resolution Times**	Incident resolution times should align to the HMRC Service Level Model - Standard Service Level Package.
9	2.9	Crowdstrike	**Configuration Management**	Adherence to HMRC's configuration management process for any configuration change to items under the scope of the agreement

Crown Commercial Service

Tenable:

10	2.10	Tenable	**Support Scope**	Responsible for monitoring, problem management and incident resolution, knowledge management, build, operational support, maintenance and patching of the underlying server and operating system that Tenable management platform and scanners are deployed on across all environments, Where deployed in cloud this will also include management of the VPC/VNET and secure configuration of the environment Responsible for ensuring latest tenable plugins and tenable updates assessed and applied in consultation with CSTS
11	2.11	Tenable	**Backup & Restore of Tooling Application**	Backup processes - Systems, schedules, restore capabilities must provide a recovery time and recovery point objective to support the service availability defined above. Back up to include OS level, Tenable application, configuration and associated scan data.
12	2.12	Tenable	**Agent Version Quality Assurance Process - Backup & Restore of Process Components**	The objective of the Tenable Agent Version Quality Assurance Process is defined in the Governance section below. Ensure the Tenable Agent Version Quality Assurance Process components (test scripts and test endpoint infrastructure builds) can be restored in the event of an outage or system change that needs to be recovered. Recovery point must be 24 hours. Recovery time must be 24 hours. The quality assurance process will involve up to ten endpoints for testing purposes. Supplier to produce Backup schedules, Backup Windows, Incremental or Full Backup, Snapshots taken beforehand, document all retention periods, roll-back and recovery process, check data integrity of backups, Testing of the Restore Process on a Quarterly basis
13	2.13	Tenable	**Agent Version Quality Assurance Process - Patching of Server Endpoints Used for Testing**	The objective of the Tenable Agent Version Quality Assurance Process is defined in the Governance section below. Ensure host machines used in the Tenable Agent Version Quality Assurance Process are correctly patched at OS level to meet HMRC security policies and standards. The Tenable Agent Version Quality Assurance Process may use up to ten test server endpoints.
14	2.14	Tenable	**Administration**	The provision of a continual scanning service that can also be used to perform scheduled and ad-hoc scanning against set policies and standard (this has the potential to be across Legacy Data Centre, Crown Hosting and Cloud Environments).

15	2.15	Tenable	Service Monitoring	The monitoring of a vulnerability assessment service across Cloud Environments, Crown Hosting and Legacy Environment. Monitoring includes ensuring the Tenable services are active, ensuring scanning is functioning as expected, reporting is functioning as expected and licence usage is compliant and communicated to business owner and IT Asset Management. Monitoring solutions should use standard HMRC Monitoring tooling. Ensure security auditing of service is maintained.
16	2.16	Tenable	Agent Versions	Ensure that only supported versions of agents are running on the estate, upgrading agent versions previously deployed where necessary and ensuring that only supported agent versions are deployed thereafter
17	2.17	Tenable	Incident Resolution Times	Incident resolution times should align to the HMRC Service Level Model - Standard Service Level Package.
18	2.18	Tenable	Infrastructure Management	Day-to-day monitoring of platform and resolution of live service issues - scope is OS tier and application tier. Tenable application on Crown needs to be supported, up and running and maintained.
19	2.19	Tenable	System Admin & Management	Technologies in scope for tooling shall be patched to latest secure and compliant versions of operating systems to align to HMRC standards & Security requirements. This includes OS tier andis the application tier. Where OS tier is dependent upon other parties, the Supplier will liaise with those parties to ensure OS tier is updated accordingly.
20	2.20	Tenable	Configuration Management	Adherence to HMRC's configuration management process for any configuration change to items under the scope of the agreement
21	2.21	Tenable	IDAM Provisioning/Management	To work with HMRC Business Owner to ensure maintenance and control of appropriate user groups/profiles through identity and access management. The approvals process to grant new users will be a HMRC function.

Tooling Maintenance

CrowdStrike:

1	3.1	CrowdStrike	Third-Party Integrations	Support, incident manage/resolve and problem manage the integration of CrowdStrike with HMRC SIEM for alerting purposes. Support, incident manage/resolve and problem manage the integration of CrowdStrike with HMRC AWS and Azure accounts for cloud discovery purposes.

				Support, incident manage/resolve and problem manage the integration of CrowdStrike within HMRC Cloud and Crown Hosting environments and teams supporting those environments.
2	3.2	CrowdStrike	**Routing/Networking**	Working collaboratively with the relevant HMRC teams to ensure end to end path availability, and required routing, firewall changes are raised to support provision of the service
3	3.3	CrowdStrike	**Vendor Engagement / Vendor Management**	Liaise with and manage the vendor of the supplied in-scope tooling, this includes management of tickets, escalation of any items which have not received attention in line with service level agreements, communication of any roadmap changes to the business owner to inform business owner decision making

Tenable:

4	3.4	Tenable	**Technical Configuration**	Responsible for build, administration, technical configuration Tenable management platform and scanners are deployed on across all environments for all types of Tenable scanning (including packaging and deployment of tenable agent)
5	3.5	Tenable	**Third-Party Integrations**	Manage the integration activity with 3rd party products - SIEM, Hashicorp Vault, Azure AD, Network Vulnerability Tooling, Service Management Tooling, Threat Intelligence Feeds, Azure, AWS. Responsible for configuration associated to integration with active directory, Hashicorp Vault to ensure access is securely maintained and provided
6	3.6	Tenable	**Patching and Security Standards**	Ensure the Tenable application servers and scanners are patched in accordance with HMRC requirements. This need to be in line with HMRC Patching Policy. Work with HMRC to support tech refresh/end of life products associated with Tenable. Ensure Tenable tooling and OS tier are compliant to the HMRC security policies, standards and procedures.
7	3.7	Tenable	**Onboarding**	The Buyer shall be responsible for onboarding and offboarding of delivery groups (up to 20 HMRC user groups) and assets (up to 20,000), along with ongoing maintenance of the end-to-end process
8	3.8	Tenable	**Routing/Networking**	Working collaboratively with the relevant HMRC teams to ensure end to end path availability, and required routing, firewall changes are raised to support provision of the service
9	3.9	Tenable	**Scaling**	Scaling of the tool - support of future enhancements and expanded use across HMRC, including packaging and deployment of agents where required to support a maximum of

				20,000 assets. Any further expansion of the solution would be under change control.
10	**3.10**	**Tenable**	**Vendor Engagement / Vendor Management**	Liaise with and manage the vendor of the supplied in-scope tooling, this includes management of tickets, escalation of any items which have not received attention in line with service level agreements, communication of any roadmap changes to the business owner to inform business owner decision making

Governance

CrowdStrike:

1	**4.1**	**Crowdstrike**	**Accessibility Compliance**	Ensure the tooling within the scope of the agreement is compliant to the latest HMRC accessibility standards, manage the vendor actions for correction to meeting accessibility compliance. Inform the HMRC business owner of any issues that would breach HMRC accessibility compliance standards.
2	**4.2**	**Crowdstrike**	**Supporting Documentation**	Ensure any required new business or technical guidance or work instructions has been produced and/or existing business or technical guidance is updated accordingly for consumption by HMRC stakeholders
3	**4.3**	**Crowdstrike**	**Change Management**	Adherence to HMRC's change management process for any change to items under the scope of the agreement
4	**4.4**	**CrowdStrike**	**Agent Version Quality Assurance Process - Execution and Agent Release**	Document and Execute the CrowdStrike Agent Quality Assurance Process to prove that candidate agent versions are compatible with representative target HMRC infrastructure and operating system build (with other monitoring agents also installed) before the candidate agent version is promoted for release to HMRC delivery groups and other distribution channels for use on the server estate. The Agent Version Quality Assurance Process should be automated and optimised to ensure best productivity. On completion of the Agent Version Quality Assurance Process, configuration changes should be made to CrowdStrike by the Supplier to allow the now proven agent version to be released to the HMRC estate (following approval from HMRC Technical Service Owner).
5	**4.5**	**CrowdStrike**	**Agent Distribution**	The provision of agents / agent packages to the following channels upon successful completion of the Agent Version Quality Assurance Process: ECS EPO distribution, ECS Cloud Server Image providers, ECS Crown Hosting Server Image Providers, Centralised Agent Repository (under Service Management and Operations ownership)
6	**4.6**	**Crowdstrike**	**Service Management Reporting and Escalation Meetings**	Monthly meeting to review service level agreements and MSP performance. Quarterly Business Reviews (QBR), Performance measured against SLA's, KPI's and Customer Satisfaction Surveys. Reporting of any Trends.

7	4.7	Crowdstrike	**Manage and Action Licence Renewals**	Manage and action the licence renewal for tooling within scope of the agreement, in accordance with HMRC commercial policies and practices, working with the HMRC commercial team to action subject to funding provision for licensing from HMRC

Tenable:

8	4.8	Tenable	**Accessibility Compliance**	Ensure the tooling within the scope of the agreement is compliant to the latest HMRC accessibility standards, manage the vendor actions for correction to meeting accessibility compliance. Inform the HMRC business owner of any issues that would breach HMRC accessibility compliance standards.
9	4.9	Tenable	**Supporting Documentation**	Ensure any required new business or technical guidance or work instructions has been produced and/or existing business or technical guidance is updated accordingly for consumption by HMRC stakeholders
10	4.10	Tenable	**Change Management**	Adherence to HMRC's change management process for any change to items under the scope of the agreement
11	4.11	Tenable	**Repository Management**	Management of Tenable data output /asset scan repositories, not management of vulnerabilities (e.g., asset scan repositories)
12	4.12	Tenable	**Agent Version Quality Assurance Process - Execution and Agent Release**	Document and Execute the Tenable Agent Quality Assurance Process to prove that candidate agent versions are compatible with representative target HMRC infrastructure and operating system build (with other monitoring agents also installed) before the candidate agent version is promoted for release to HMRC delivery groups and other distribution channels for use on the server estate. The Agent Version Quality Assurance Process should be automated and optimised to ensure best productivity. On completion of the Agent Version Quality Assurance Process, configuration changes should be made to Tenable by the Supplier to allow the now proven agent version to be released to the HMRC estate (following approval from HMRC Technical Service Owner).
13	4.13	Tenable	**Agent Distribution**	The provision of agents / agent packages to the following channels upon successful completion of the Agent Version Quality Assurance Process: ECS Crown Hosting Server Image Providers, Centralised Agent Repository
14	4.14	Tenable	**Service Management Reporting and Escalation Meetings**	Monthly meeting to review service level agreements and MSP performance. Quarterly Business Reviews (QBR), Performance measured against SLA's, KPI's and Customer Satisfaction Surveys. Reporting of any Trends.
15	4.15	Tenable	**Manage and Action Licence Renewals**	Manage and action the licence renewal for tooling within scope of the agreement, in accordance with HMRC commercial policies and practices, working with the HMRC commercial team to action subject to funding provision for licensing from HMRC

Crown Commercial Service

Platform Scope

CrowdStrike:

1	5.1	CrowdStrike	Platform Scope	The CrowdStrike Platform scope is a SaaS solution provided by CrowdStrike, servicing server endpoints utilising up to 84m compute hours over a 3-year profile. Integration points are noted elsewhere in these requirements. The core IT functions and integrations for the CrowdStrike solution will be in place before this agreement commences.

Tenable:

2	5.2	Tenable	Platform Scope	The Tenable Platform scope is an on-prem and cloud solution initially built by HMRC servicing up to approx. 20,000 server endpoints and approx. 2,500 Desktop endpoints. The platform will include up to 3 management servers, 3 scanners in LDC, 5 scanners in CH, 2 scanners in cloud and 2 scanners in Sysman, with potential for deployment of additional scanners to accommodate future scanning requirements and coverage. The 2 Sysman scanners are a tactical solution and will be decommissioned later in the year Integration points are noted elsewhere in these requirements. The core IT functions and integrations for the Tenable solution will be in place before this agreement commences. Plus development/maintenance of either Non-Production environment.

Crown Commercial Service

Service Levels

The Supplier will be subject to KPI measurement defined in the HMRC Service Level Model – Standard Service Level Package, full details of which can be found in the Event Attachments.
The HMRC Standard Service Level Model is, at a high-level, as follows:

Support Hours	07:00-19:00
Hours Per Day	12
Supported Days	**MTWTF**~~SS~~
Bank Holidays	No
Availability Targets	**99%**

The HMRC Standard Service Level Model defines the following Incident Resolution KPIs:

Standard
P1: **4Hrs** P2: **8Hrs** P3: **1 Day** P4: **3 Days** P5: **5 Days**

All tasks within the Specified Objectives, including monitoring, cannot be affected by Incident Resolution The Supplier will provide an indicative service delivery plan as part of their proposal. Any changes to the plan must be agreed within 14 days of the call-off commencement date and must be agreed by both parties in writing.

1.7 Continuous Improvement

1.7.1 The Supplier must, throughout the Contract Period, identify new or potential improvements to the provision of the Deliverables with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables and their supply to the Buyer.

1.7.2 The Supplier must adopt a policy of continuous improvement in relation to the Deliverables, which must include regular reviews with the Buyer of the Deliverables and the way it provides them, with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables. The Supplier and the Buyer must provide each other with any information relevant to meeting this objective.

1.7.3 HMRC encourages upskilling and would also expect the Supplier to provide knowledge transfer within delivery of the requirements in addition to demonstrating innovative ideas and value-added initiatives.

1.8 Location

1.8.1 Given the current restrictions due to COVID-19, the Supplier will need to work virtually to begin with. The specifics of how this will be handled will be discussed with the Supplier upon contract commencement.

1.8.2 Once measures have been relaxed the primary locations will be……

- HMRC Stratford, London
- Benton Park View, Newcastle
- Plaza 2, Telford
- Trinity Bridge House, Salford
- 7&8 Wellington Place, Leeds

1.8.3 As part of the delivery, for example to conduct stakeholder workshops and meetings, it may be necessary for the Supplier to travel to other HMRC sites upon request.

1.9 Security

1.9.1 Supplier staff to deliver these services will need vetting and Full Security Clearances must be held prior to the Contract Start Date.

1.9.2 The Supplier will be required to comply with the HMRC's Security and vetting requirements which will be determined by the HMRC Security Information Business Partner, but SC clearance will be the expected default for the Service Provider's staff that will be engaged in the contract.

1.9.3 In the delivery of the service, the Service Provider must ensure that the standards, best practice guidelines and approaches that are required to protect UK government assets contained in the Security Policy Framework are adhered to.

1.9.4 The Supplier's response to the Security Questionnaire, with any subsequent amendments as may be agreed as part of a clarification process, will be included in the signed version of any resulting agreement, as confirmation that the content of the Security Plan has been agreed with HMRC.

1.9.5 The Service Provider shall ensure that all personnel (employees, sub-contractors, associates etc.) providing services have been checked in accordance with the HMG Security Check (SC) Standards. Successful Service Provider will be asked to provide further assurance prior to the Contract Commencement date.

1.9.6 Where additional personnel are provided, or personnel are replaced during the contract the Service Provider will assure that the relevant checks are in place for the additional/replacement personnel.

Confidentiality

An HMRC standard Non-Disclosure Agreement (NDA) may be required to be signed by the suppliers invited to tender at any stage during the procurement process.

1.10 Expenses

1.10.1 Given that most of the work should be able to be completed at HMRC's primary locations only, additional Travel and Subsistence expenses will not be paid and must be accounted for as part of the base charge proposal.

1.10.2 Should excessive requests be made of the Supplier to travel to other HMRC sites then Travel and Subsistence expenses will only be paid with the prior agreement of the HMRC Work Manager.

1.10.3 Any expenses agreed to by the HMRC Works Manager must be in compliance with HMRC travel & subsistence policy, which will be provided at the time of the request.

1.10.4 All other expenses/disbursements will be payable at the discretion of the HMRC Work Manager. The Supplier shall not incur any such expenses without the prior approval of the HMRC Work Manager. Any expense incurred by the Supplier without prior approval shall not be reimbursed.

1.11 Invoicing

1.11.1 Prior to invoicing, acceptance and approval must be sought from the HMRC employee responsible for managing and approving the work (the Work Manager)

1.11.2 Under no circumstances should the aggregated total value of invoices, including the proposed value of your final invoice, exceed the amount stated in the signed contract, unless additional work has subsequently been agreed in writing as a formal contract variation.

1.11.3 Invoicing will be conducted via HMRC's eTrading system provided by SAP Ariba (further information can be found in the HMRC Tendering Instructions document).

Crown Commercial Service

Clarification Questions Log

The Buyer has provided the following clarifications to the above requirements:

Tender Clarification Record: EDR and Vulnerability Managed Service SR788241953					
Document Version No.V1.0			**Version Issue Date: 17/05/2022**		
Information which has been added in this latest version are highlighted in yellow. Previously answered questions are shaded blue.					
Question Number	**Version**	**Topic**	**Question**	**Answer**	**Ariba Message Ref**
Q001	V1.0	Service Levels & KPI's	Please provide any required KPI's in relation to deliverables 4.6 / 4.14	The '9. HMRC Service Level Model' in the event attachments provides general service levels with specific KPIs to be agreed at contract finalisation stage.	MSG96772204
Q002	V1.0	Specification	Does the service scope include delivery of the migration and decomm of the tactical solution (2x tenable sysman scanners) or is this an extra scope, potenially via Change Requests? (Deliverable 5.2)	Not included in service scope.	MSG96772204
Q003	V1.0	Responsibilities	What is the expected scope of activities for onboarding delivery groups into Tenable and who is responsible for each action (Deliverable 3.7)? If changes are required on endpoints, how is this activity engaged?	This will be carried out by HMRC.	MSG96772204

Q004	V1.0	Responsibilities	In order to help qualify the upskill requirement, is there any further information available on the expected roles and responsibilities for the on-going advisory role? Deliverable 1.4	As per the requirement, upskilling will be expected when there are any updates or changes within the Crowdstrike system. This isn't specific to one user role and will be appropriate for the whole team with Crowdstrike access.	MSG96772204

Q005	V1.0	TUPE	On the assumption TUPE applies based on information in the RFP, please provide the below information anonymised and in table format for each employee: 1. How many staff in scope (including any sub-contractors) – we assume 5 as per the RFP but would appreciate a confirmation of numbers, 2. Who is their current employer? We assume HMRC but would appreciate a confirmation, 3. Salary for each, 4. Hours that each do per week and the FTE per week, 5. Are any from a previous TUPE, if so which ones and who was the previous organisation, 6. Any benefits for each and amount, 7. What pension scheme are they in and what is the employer contribution (we assume Civil Service pension scheme, but would appreciate a confirmation), 8. Length of service, 9. Age, 10. Employer Notice period, 11. Continuous service start date, 12. Job role and percentage of role doing the work that is proposed to be transferred, 13. Redundancy terms, 14. Does anyone have Beckmann rights or other enhanced rights, if so who?, 15. Contractual base location for each role, 16. Any collective agreements in place and if so what are they and who do they apply to, 17. Pay arrangements, 18. Any protected pay arrangements, 19. Any outstanding pay award – if so what is it, 20. Job Spec per employee, 21. Any current claims/ disciplinary proceedings/ grievance proceedings.	We do not feel TUPE is applicable as current service providers are contingent labour staff paid a daily rate so no salary, benefits, pension, redundancy terms, etc.,. However, for transparency and to allow bidders to make their own informed decisions, we have provided staff details in the event attachment 'HMRC - TUPE info (Anomynised)'	MSG96772204

Q006	V1.0	Responsibilities	Assuming the managed service provider is only responsible for monitoring Crowdstrike agents after they have been enrolled are you able to share the enrollment process and who is responsible for managing this programme of work?	Onboarding will be conducted inhouse by the project team. This process will be explained at contract stage.	MSG96772204
Q007	V1.0	Responsibilities	Assuming the managed service provider is only responsible for monitoring for successful vulnerability scans based on the to be agreed criteria after they have been enrolled are you able to share the enrollment process and who is responsible for managing this programme of work?	Onboarding will be conducted inhouse by the project team. This process will be explained at contract stage.	MSG96772204
Q008	V1.0	Responsibilities	Assuming the managed service provider isn't responding to any security events generated by the Crowdstrike tooling are you able to advise who will be responsible for this?	This is the responsibility of the HMRC Cyber Security team.	MSG96772204
Q009	V1.0	Responsibilities	Assuming the managed service provider isn't responding to any security events generated by the Crowdstrike tooling who will be responsible for amending and updating any Crowdstrike policies?	Any policy updates will be conducted by HMRC, the MSP team will not be required to do this	MSG96772204
Q010	V1.0	Responsibilities	Will HMRC manage the license arrangements for Nessus and Crowdstrike and provide Fujitsu the ability to arrange support calls and have account contacts with the vendors?	HMRC will manage all license arrangements; conduct and engagement with the vendor will be the responsibility of the MSP and HMRC will provide the MSP the ability to do this.	MSG96772204
Q011	V1.0	Specification	In order to help qualify the upskill requirement , is there any further information available on the scope of the Tenable system Training Plan? Deliverable 1.10	As per the requirement, upskilling will be expected for delivery group users of Tenable and for HMRC Cyber Security Technical Services team.	MSG96772204
Q012	V1.0	Budget	Please can you confirm the estimated budget and how it was calculated?	The budget was calculated against current costs and expected increase in activity over the contract period	MSG96804170

Q013	V1.0	TUPE	The RFP states that the service is currently being delivered by a team of 5. Please can you share which organisation(s) these team members work for and if you believe TUPE may apply?	We do not feel TUPE is applicable as current service providers are contingent labour staff paid a daily rate so no salary, benefits, pension, redundancy terms, etc.,. However, for transparency and to allow bidders to make their own informed decisions, we have provided staff details in the event attachment 'HMRC - TUPE info (Anonymised)'	MSG96804170
Q014	V1.0	Location	Would you be willing to consider the service being delivered remotely?	Yes, with the caveat that some IT engineering work has to be done on HMRC premises and connection as it can't be accessed remotely, so there would have to be a hybrid working method.	MSG96804170
Q015	V1.0	Specification	The RFP includes details of support hours. Please can you confirm if any out of hours support will be required and, if so, what these requirements are?	No out of hours support is required.	MSG96804170
Q016	V1.0	Specification	Please can you provide details of how this requirement fits within the wider service model?	The Managed Service would sit within the Service Management and Operations (SM&O) in Chief Digital and Information Office (CDIO), interactions with other teams can be discussed further during contract finalisation.	MSG96804170
Q017	V1.0	Service Levels & KPI's	Can HMRC please share the current the service level agreements for Crowdstrike? We will need to align any services we provide to the service level agreements between HMRC and the vendor	This information is in the event attachment 'CrowdStrike Operational Support Model'.	MSG96772235
Q018	V1.0	Responsibilities	Will there be a requirement for us to manage and operate the infrastructure, in particular with reference to the Tenable tool, that the solution is based on? i.e. patching of the operating system etc?	No	MSG96772235
Q019	V1.0	Specification	How is the system availability currently monitored?	Crowdstrike is monitored via a SAS console, alerts and notifications will be received if there are any errors/downtime. Tenable - the tenable deployment is still in a test environment so is currently being monitored by the project team	MSG96772235

Q020	V1.0	Tools	Please provide a list of the tools which HMRC mandate are used for support activities (e.g. ServiceNow)	ServiceNow	MSG96772235
Q021	V1.0	Specification	Is the user provisioning for the in-scope systems linked to AD via the normal HMRC identity management service for management of users or will this be a manual process within the tools themselves?	This is a manual task that will be performed by HMRC.	MSG96772235
Q022	V1.0	Specification	What is the likely audience for training / up-skilling (e.g. functions, job roles)?	Cyber Security Teams and key stakeholders in delivery groups.	MSG96772235
Q023	V1.0	Specification	Could you please provide more information on the reporting requirements for each of the solutions e.g. nature of reports and frequency?	Weekly checkpoints with CrowdStrike/Tenable and Cyber Security Teams Monthly Service Review with CrowdStrike/Tenable Weekly Status reports.	MSG96772235
Q024	V1.0	Responsibilities	Are we correct in assuming that the contracts with the suppliers will remain with HMRC and there is no intention to novate these to the provider of the managed service?	Yes this is correct	MSG96772235
Q025	V1.0	Location	Would HMRC consider the provision of the managed service from a single UK based location rather than out of the named HMRC Security locations?	This is an option and detail of conditions are in the Security Policy Framework.	MSG96772235
Q026	V1.0	TUPE	Could HMRC please confirm whether TUPE in in scope for this opportunity in relation to the internal resources currently delivering this service for HMRC?	We do not feel TUPE is applicable as current service providers are contingent labour staff paid a daily rate so no salary, benefits, pension, redundancy terms, etc.,. However, for transparency and to allow bidders to make their own informed decisions, we have provided staff details in the event attachment 'HMRC - TUPE info (Anonymised)'	MSG96723231

Q027	V1.0	Commercial	We assume that the order form will be completed post award, and therefore we do not need to supply as part of our tender response?	That is correct	MSG96810201
Q028	V1.0	Security	Please can you confirm the level of security clearance staff will require?	As noted in 3.10.1 Full Security Clearance (SC) is re-quired.	MSG96810201

For the purposes of this agreement CQ18 in the log above shall be disregarded.

Crown Commercial Service

The Service to be provided by the Supplier is based upon the following metrics provided by the Buyer:

RFP Scope	Volume
Tenable licences	20,000
Crowdstrike	15,000
Tenable Management Servers (Production)	3
Tenable Scanners (Production)	12
Operating system support	0
OS Versions for which Agents are deployed	10
5 Prod EC2 instances – Tenable.SC (RHEL), Nessus Manager (RHEL), 2x Nessus Scanners (RHEL), Windows Jump box (Windows)	
14 Dev EC2 instances – Tenable.SC (RHEL), Nessus Scanner (RHEL), Windows host server (Windows), RHEL host server (RHEL) & 10 unknown Crowdstrike QA payloads	
platform incident rate of 2 per month and patching taking place once a month during service hours.	
General EC2 management are a maximum of 5 occasions per year	

Should the volumes set out above be exceeded, the implications shall be reviewed in accordance with the Change Control Procedure.

Buyer Responsibilities:
The following are Buyer Responsibilities:

Responsibility No.	Responsibility description
1	Tenable and Crowdstrike agents able to be updated via the management console
2	The Buyer CrowdStrike solution shall be in place before this agreement commences
3	The Buyer shall: • maintain support contracts with vendors (Crowdstrike & Tenable) in line with the HMRC Standard Service Level Package • agree with the applicable vendor that the Supplier can operationally act on the Buyer's behalf • act as an escalation point where required
4	The Buyer shall provide existing knowledge articles and processes and provide access to Crowdstrike University,

5	The Buyer shall be responsible for the onboarding of new devices to the Crowdstrike and Tenable solutions, and informing the Supplier of such onboarding.
6	The Buyer shall manage patching of Operating Systems to be at a level required for the Crowdstrike and Tenable solutions.
7	The Buyer shall manage network related activities to enable the provision of the Services
8	The Buyer shall provide the Supplier with all access required and all tools to be able to manage these payloads in accordance to HMRC policy

Crown Commercial Service

Attachment 2 – Charges and Invoicing

Part A – Milestone Payments and Delay Payments

NOT USED

Part B – Service Charges

Total Fixed Price - Year 1	*REDACTED*
Total Fixed Price - Year 2	*REDACTED*
Total 2 year Fixed Price	*REDACTED*

REDACTED

Crown Commercial Service

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

SFIA Rate Levels: Refer to SFIA Skills Model 7.0 https://sfia-online.org/en

	SFIA Role	3	4	5	6
		Day rate (£)	Day rate (£)	Day rate (£)	Day rate (£)
Development and Implementation	Systems Integration and Build	REDACTED	REDACTED	REDACTED	REDACTED
Delivery and Operation	Service Level Management	REDACTED	REDACTED	REDACTED	REDACTED
Skills and Quality	Learning and Development Management	REDACTED	REDACTED	REDACTED	REDACTED
Relationship and Engagement	Customer Service Support	REDACTED	REDACTED		
	Relationship Management			REDACTED	REDACTED

Note: Where the Buyer requests management of security groups and troubleshooting of issues, this will be charged at the applicable rate in line with the Rate Card set out above.

Part D – Risk Register

NOT USED

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6	Column 7	Column 8	Column 9	Column 10	Column 12
Risk Number	Risk Name	Description of risk	Timing	Likelihood	Impact (£)	Impact (description)	Mitigation (description)	Cost of mitigation	Post-mitigation impact (£)	Owner

Part E – Early Termination Fee(s)

Not Applicable

Crown Commercial Service

Attachment 3 – Outline Implementation Plan

REDACTED

Crown Commercial Service

Attachment 4 – Service Levels and Service Credits

Service Levels

The Supplier will be subject to KPI measurement defined in the HMRC Service Level Model – Standard Service Level Package, full details of which can be found in the Event Attachments.

9. HMRC Service Level Model.xlsx

The HMRC Standard Service Level Model is, at a high-level, as follows:

Support Hours	07:00-19:00
Hours Per Day	12
Supported Days	**MTWTFSS**
Bank Holidays	No
Availability Targets	**99%**

The HMRC Standard Service Level Model defines the following Incident Resolution KPIs:

Standard
P1: **4Hrs** P2: **8Hrs** P3: **1 Day** P4: **3 Days** P5: **5 Days**

All tasks within the Specified Objectives, including monitoring, cannot be affected by Incident Resolution

The Supplier will provide an indicative service delivery plan as part of their proposal. Any changes to the plan must be agreed within 14 days of the call-off commencement date and must be agreed by both parties in writing.

A Service credit mechanism will be agreed between the parties prior to commencement of the contract when service levels above have not been met.

Service Levels							Service Credits
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Target**	**Service Level Failure Threshold (Minor)**	**Service Level Failure Threshold (Major)**	**Service Level Failure Threshold (Critical)**	**Service Points**
(KPI 1-1) P1 Priority Incident "Incident Resolution Threshold In Support Hours only Measured within Supported Hours on Supported Days, Between the States of New & Resolved"	Resolution	Less than 4 hours	No more than 1 P1 fail	More than 1 P1 Incident fails the target	More than 2 P1 Incidents fail the target	N/A	20 Points for ANY Minor Failure 30 Points for ANY Major Failure
(KPI 1-2) P2 Priority Incident "Incident Resolution Threshold In Support Hours only Measured within Supported Hours on Supported Days, Between the States of New & Resolved"	Resolution	Less than 8 hours	No more than 2 P2 fails	More than 2 P1 Incident fails the target	More than 4 P1 Incidents fail the target	N/A	
(KPI 1-3) P3 Priority Incident "Incident Resolution Threshold In Supported Hours only Measured within Supported Hours on Supported Days, Between the States of New & Resolved"	Resolution	Less than 1 Day	>= 20 Incidents – 85% of Incidents Achieve Target OR <20 Incidents - No more than 3 P3 fails	More than 15% of P3 Incidents fail the target OR More than 3 P3 Incidents fail the target	More than 20% of P3 Incidents fail the target OR More than 4 P3 Incidents fail the target	N/A	
(KPI 1-4) P4 Priority Incident "Incident Resolution Threshold In Supported Hours only Measured within Supported Hours on Supported Days, Between the States of New & Resolved"	Resolution	Less than 3 Day	>= 20 Incidents – 90% of Incidents Achieve Target OR <20 Incidents - No more than 2 P4 fails	More than 10% of P4 Incidents fail the target OR More than 2 P4 Incidents fail the target	More than 15% of P4 Incidents fail the target OR More than 3 P4 Incidents fail the target	N/A	
(KPI 1-5) P5 Priority Incident "Incident Resolution Threshold In Supported Hours only	Resolution	Less than 5 Day	>= 20 Incidents – 95% of Incidents Achieve Target OR	More than 5% of P5 Incidents fail the target OR	More than 10% of P5 Incidents fail the target OR	N/A	

Measured within Supported Hours on Supported Days, Between the States of New & Resolved"			<20 Incidents - No more than 1 P5 fails	More than 1 P5 Incident fails the target	More than 2 P5 Incidents fail the target		
Service Levels							**Service Credits**
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Target**	**Service Level Failure Threshold (Minor)**	**Service Level Failure Threshold (Major)**	**Service Level Failure Threshold (Critical)**	**Service Points**
(KPI 2-1) Availability Threshold Percentage Measured within Supported Hours/Days over a calendar Month (Example Outage Threshold equivalent to 2 Hours 24 Minutes over a Calendar Month which includes 20 Supported Days)	Individual Service Availability	Any Individual Service >= 99.00%	Any Individual Service >= 99.00% Service Availability achieved in the period	Any Individual Service < 99.00% Availability achieved in the period	Any Individual Service < 98.00% Availability achieved in the period	Any Individual Service < 97.00% Availability achieved in the period	20 Points for Minor Failure 30 Points for Major Failure 40 Points for Critical Failure
(KPI 3-1) Problem assessment for P1, 2, 3, 4 Problems "Problem Assessment Threshold In Days, Measured on a Mon-Fri, 08:00 to 18:00 Basis, No Holiday Support, Between the States of New and reaching RCA State"	Response	5 Days on a Mon-Fri, 08:00 to 18:00 Basis No Holiday Support	>= 20 Problems – 95% of P1 to P4 Problems Assessed Within Target OR <20 Problems - No more than 2 fails	> 5% of P1 to P4 Problems fail the Assessment target OR More than 2 Problems fail the target	> 10% of P1 to P4 Problems fail the Assessment target OR More than 3 Problems fail the target	N/A	10 Points for Minor Failure 20 Points for Major Failure
(KPI 4-1) Problem Resolution for P1 & P2 Problems "Problem Resolution Threshold In Months, Measured on a Mon-Fri, 08:00 to 18:00 Basis, No Holiday Support, Between the States of RCA and reaching Resolved State"	Resolution	3 Months (65 Days) (650 Hours) on a Mon-Fri 08:00 to 18:00 Basis No Holiday Support	>= 20 Problems - >= 90% of P1 & P2 Problems Resolved within target OR < 20 Problems - No more than 2 P1 or P2 Fails	> 10% of P1 & P2 Problems fail the Resolution target OR More than 2 P1 or P2 Problems fail the target	> 15% of P1 & P2 Problems fail the Resolution target OR More than 3 P1 or P2 Problems fail the target	N/A	10 Points for ANY Minor Failure 20 Points for ANY Major Failure
(KPI 4-2) Problem Resolution for P3 & P4 Problems "Problem Resolution Threshold	Resolution	6 Months (130 Days) (650 Hours) on a Mon-Fri	>= 20 Problems - >= 90% of P3 & P4 Problems Resolved within target	> 10% of P3 & P4 Problems fail the	> 15% of P3 & P4 Problems fail the	N/A	

In Months, Measured on a Mon-Fri, 08:00 to 18:00 Basis, No Holiday Support, Between the States of RCA and reaching Resolved State"		08:00 to 18:00 Basis No Holiday Support	OR < 20 Problems - No more than 2 P3 or P4 Fails	Resolution target OR More than 2 P3 or P4 Problems fail the target	Resolution target OR More than 3 P3 or P4 Problems fail the target		

Service Levels							Service Credits
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Target**	**Service Level Failure Threshold (Minor)**	**Service Level Failure Threshold (Major)**	**Service Level Failure Threshold (Critical)**	**Service Points**
(KPI 5-1) Change Enablement To ensure that all Change, especially service impacting change, is processed appropriately, with all governance and due diligence activities being completed to prevent loss of service to the customer	Change Quality	Zero P1 or P2 Incidents Caused by Change	Zero	>0 P1 or P2 Incidents Caused by Change	>1 P1 or P2 Incidents Caused by Change	N/A	10 Points for Minor Failure 20 Points for Major Failure
(KPI 6-1) To Produce and issue a Patch Compliance Report for each Reporting Period, by Working Day 3 of the following month, providing the patch compliance status of all agreed assets to HMRC patch Policy	Timeliness	On or before Working Day 3, following the end of the Reporting Period	<= Working Day 3, following the end of the Reporting Period	> Working Day 3, following the end of the Reporting Period	> Working Day 7, following the end of the Reporting Period	N/A	5 Points for Minor Failure 20 Points for Major Failure
(KPI 7-1) Expedited security patches being applied in a timely manner Note: Patching activity is not limited to Scheduled Hours	Timeliness	No (Zero) critical security patches outstanding after 14 days, or the agreed implementation timescales.	None (Zero) Outstanding	> 0 (Zero) Outstanding	> 2 Outstanding	Any vulnerability to be addressed by any agreed but unimplemented urgent security patch has been exploited within HMRC; and such exploitation causes a significant security breach	10 Points for Minor Failure 20 Points for Major Failure 30 Points for Critical Failure

Crown Commercial Service

Service Levels							Service Credits
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Target**	**Service Level Failure Threshold (Minor)**	**Service Level Failure Threshold (Major)**	**Service Level Failure Threshold (Critical)**	**Service Points**
(KPI 8-1) To produce and issue a Vulnerability Assessment Report for each Reporting Period, by Working Day 3 of the following month, providing the vulnerability assessment of all agreed Assets, Systems & Services to HMRC policy	Timeliness	On or before Working Day 3, following the end of the Reporting Period	<= Working Day 3, following the end of the Reporting Period	> Working Day 3, following the end of the Reporting Period	> Working Day 7, following the end of the Reporting Period	N/A	5 Points for Minor Failure 20 Points for Major Failure
(KPI 9-1) Adherence to agreed Mitigation & Remediation timescales by Severity Level to HMRC Policy Note: Mitigation & Remediation activities are not restricted to within Scheduled hours, and should be considered as 24/7/365 activities where required in the policy	Timeliness	To agreed timescales for each Severity Level	No (Zero) failures to achieve Mitigation or Remediation timescales	> 0 (Zero) failures to achieve Mitigation or Remediation timescales	> 2 failures to achieve Mitigation or Remediation timescales	> 5 failures to achieve Mitigation or Remediation timescales	10 Points for Minor Failure 20 Points for Major Failure 30 Points for Critical Failure

The Supplier shall not be deemed to have failed a KPI or Service Level, where the failure is as a result of the Buyer or a Buyer third party.

Summary Table of Minor, Major & Critical Service Credit Points per KPI

KPI	Minor Service Points	Major Service Points	Critical Service Points
KPI 1 - Incident Management	20	30	N/A
KPI 2 - Service Availability	20	30	40
KPI 3 - Problem Assessment	10	20	N/A
KPI 4 - Problem Resolution	10	20	N/A
KPI 5 - Change Enablement	10	20	N/A
KPI 6 - Patch Reporting	5	20	N/A
KPI 7 - Patch Timeliness	10	20	30
KPI 8 - Vulnerability Reporting	5	20	N/A
KPI 9 - Mitigation & Remediation	10	20	30
Contract Total	**100 (Max 100)**	**200 (Max 200)**	**100 (Max 200)**
Per KPI	**Max Per KPI = 25**	**Max Per KPI = 35**	**Max Per KPI = 45**

Crown Commercial Service

Note: Service Points can be redistributed at the discretion of the Buyer with 1 Calendar Months' Notice, within the maximum limits of 100 Minor Points. 200 Major Points and 200 Critical Points, and also within the Maximum Points per KPI
If three (3) Major Failures occur in any consecutive Six (6) month period, this will be considered a Critical Failure Event, and the Buyer reserves the right to introduce additional Critical Level Points within the 200 Points maximum, for any KPI currently without a Critical Points value.

Service Credit Cap

The Service Credit Cap is 15% of the Monthly Contract Value

Service Credit Calculation: (Example)

SC = ((TSP x %) x (SCC)) x AC

		Example Figures		Example Result
SC =	*Service Credit - is the total Service Credit calculated for the relevant Service Period; and payable by the supplier*		=	**£15,000**
TSP =	*Total Service Points - is the total Service Points that have accrued for the relevant Service Period for ALL KPI failures*	= 20		
% =	*is 1% (Effectively 1% per Service Point)*	= 1.00%		
SCC =	*Service Credit Cap - is the Service Credit Cap agreed for the contract*	= 15.00%	= £75,000.00	
AC =	*Account Charge - is the total Contract Value payable for the relevant Service Period*	= £500,000.00		

Calculation: **SC = ((TSP x %) x (SCC)) x AC**

Equates to: **£15,000 = ((20 x 1%) x (15%)) x 500,000**

Therefore: Using the 20 Service Points, the Account Charge and the Service Credit Cap in the example, this KPI failure would generate a Service Credit of £15,000, this is below the Cap of £75,000, so **£15,000** would be payable in full

If more than one KPI were to fail in a period, the total Service Credit Points added together, would be used in the calculation

Report submission:
The Supplier will be required to submit their performance report for the period, in a format defined by the Buyer, within 10 Working Days following the end of the reporting period.

Note: For a period covering one month after the service commencement date, the Supplier shall monitor the service performance, however in that initial month, Service Credits shall not apply and shall not be payable.

Crown Commercial Service

Attachment 5 – Key Supplier Personnel and Key Sub-Contractors

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

Part A – Key Supplier Personnel

This section is currently Not Applicable

Key Supplier Personnel	Key Role(s)	Duration
		[*Contract Period or insert alternative timescale*]
		[*Contract Period or insert alternative timescale*]
		[*Contract Period or insert alternative timescale*]

Part B – Key Sub-Contractors

Not Applicable

Crown Commercial Service

Attachment 6 – Software

The Software below is licensed to the Buyer in accordance with Clauses 20 (*Intellectual Property Rights*) and 21 (*Licences Granted by the Supplier*).

The Parties agree that they will update this Attachment 6 periodically to record any Supplier Software or Third Party Software subsequently licensed by the Supplier or third parties for the purposes of the delivery of the Services.

Part A – Supplier Software

This section is currently Not Applicable

The Supplier Software includes the following items:

Software	Supplier (if an Affiliate of the Supplier)	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/ Expiry

Crown Commercial Service

Part B – Third Party Software

This section is currently Not Applicable

The Third Party Software shall include the following items:

Third Party Software	Supplier	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/ Expiry

Attachment 7 – Financial Distress

Not Applicable

Attachment 8 – Governance

Not Applicable

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

Not Applicable

Attachment 10 – Transparency Reports

Not Applicable

Title	Content	Format	Frequency
[Performance]			
[Charges]			
[Key Sub-Contractors]			
[Technical]			
[Performance management]			

Attachment 11 – Fujitsu Submission to Questions 3.2.1 to 3.2.7 and 3.3.1

REDACTED

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

HM Revenue & Customs

S10: HMRC Authority Mandatory Terms

AUTHORITY'S MANDATORY TERMS

A. For the avoidance of doubt, references to 'the Agreement' mean the attached Call-Off Contract between the Supplier and the Authority. References to 'the Authority' mean 'the Buyer' (the Commissioners for Her Majesty's Revenue and Customs).

B. The Agreement incorporates the Authority's mandatory terms set out in this Schedule S10: HMRC Authority Mandatory Terms.

C. In case of any ambiguity or conflict, the Authority's mandatory terms in this S10: HMRC Authority Mandatory Terms will supersede any other terms in the Agreement.

D. For the avoidance of doubt, the relevant definitions for the purposes of the defined terms set out in the Authority's mandatory terms in this Schedule S10: HMRC Authority Mandatory Terms are the definitions set out at Clause 1 of this Schedule S10: HMRC Authority Mandatory Terms

1. Definitions

"Affiliate"	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time;
"Authority Data"	the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are: supplied to the Supplier by or on behalf of the Authority; and/or which the Supplier is required to generate, process, store or transmit pursuant to this Agreement; or any Personal Data for which the Authority is the Controller, or any data derived from such Personal Data which has had any designatory data identifiers removed so that an individual cannot be identified;
"Charges"	the charges for the Services as specified in Attachment 2 – Charges and Invoicing;
"Connected Company"	means, in relation to a company, entity or other person, the Affiliates of that company, entity or other person or any other person associated with such company, entity or other person;
"Control"	the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and "Controls" and "Controlled" shall be interpreted accordingly;

"Controller", "Processor", "Data Subject",	take the meaning given in the UK GDPR;
"Data Protection Legislation"	(a) "the data protection legislation" as defined in section 3(9) of the Data Protection Act 2018; and; (b) all applicable Law about the processing of personal data and privacy;
"Key Subcontractor"	any Subcontractor: which, in the opinion of the Authority, performs (or would perform if appointed) a critical role in the provision of all or any part of the Services; and/or with a Subcontract with a contract value which at the time of appointment exceeds (or would exceed if appointed) ten per cent (10%) of the aggregate Charges forecast to be payable under this Call-Off Contract;
"Law"	any applicable Act of Parliament, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of section 2 of the European Communities Act 1972, regulatory policy, guidance or industry code, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply;
"Personal Data"	has the meaning given in the UK GDPR;
"Purchase Order Number"	the Authority's unique number relating to the supply of the Services;
"Services"	the services to be supplied by the Supplier to the Authority under the Agreement, including the provision of any Goods;
"Subcontract"	any contract or agreement (or proposed contract or agreement) between the Supplier (or a Subcontractor) and any third party whereby that third party agrees to provide to the Supplier (or the Subcontractor) all or any part of the Services, or facilities or services which are material for the provision of the Services, or any part thereof or necessary for the management, direction or control of the Services or any part thereof;
"Subcontractor"	any third party with whom: the Supplier enters into a Subcontract; or a third party under (a) above enters into a Subcontract, or the servants or agents of that third party;
"Supplier Personnel"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor of the Supplier engaged in the performance of the Supplier's obligations under the Agreement;
"Supporting Documentation"	sufficient information in writing to enable the Authority to reasonably verify the accuracy of any invoice;
"Tax"	all forms of tax whether direct or indirect;

national insurance contributions in the United Kingdom and similar contributions or obligations in any other jurisdiction;

all statutory, governmental, state, federal, provincial, local government or municipal charges, duties, imports, contributions. levies or liabilities (other than in return for goods or services supplied or performed or to be performed) and withholdings; and

any penalty, fine, surcharge, interest, charges or costs relating to any of the above,

in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction;

"Tax Non-Compliance"	where an entity or person under consideration meets all 3 conditions contained in the relevant excerpt from HMRC's "Test for Tax Non-Compliance", as set out in Annex 1, where: the "Economic Operator" means the Supplier or any agent, supplier or Subcontractor of the Supplier requested to be replaced pursuant to Clause **Error! Reference source not found.**; and any "Essential Subcontractor" means any Key Subcontractor;
"UK GDPR"	the UK General Data Protection Regulation, the retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679);
"VAT"	value added tax as provided for in the Value Added Tax Act 1994.

2. Payment and Recovery of Sums Due

2.1 The Supplier shall invoice the Authority as specified in Attachment 2 – Charges and Invoicing of the Agreement. Without prejudice to the generality of the invoicing procedure specified in the Agreement, the Supplier shall procure a Purchase Order Number from the Authority prior to the commencement of any Services and the Supplier acknowledges and agrees that should it commence Services without a Purchase Order Number:

2.1.1 the Supplier does so at its own risk; and

2.1.2 the Authority shall not be obliged to pay any invoice without a valid Purchase Order Number having been provided to the Supplier.

2.2 Each invoice and any Supporting Documentation required to be submitted in accordance with the invoicing procedure specified in the Agreement shall be submitted by the Supplier, as directed by the Authority from time to time via the Authority's electronic transaction system.

2.3 If any sum of money is recoverable from or payable by the Supplier under the Agreement (including any sum which the Supplier is liable to pay to the Authority in respect of any breach of the Agreement), that sum may be deducted unilaterally by the Authority from any sum then due, or which may come due, to the Supplier under the Agreement or under any other agreement or contract with the Authority. The Supplier shall not be entitled to assert any credit, set-off or counterclaim against the Authority in order to justify withholding payment of any such amount in whole or in part.

3. Warranties

3.1 The Supplier represents and warrants that:

3.1.1 in the three years prior to the Effective Date, it has been in full compliance with all applicable securities and Laws related to Tax in the United Kingdom and in the jurisdiction in which it is established;

3.1.2 it has notified the Authority in writing of any Tax Non-Compliance it is involved in; and

3.1.3 no proceedings or other steps have been taken and not discharged (nor, to the best of its knowledge, are threatened) for the winding up of the Supplier or for its dissolution or for the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Supplier's assets or revenue and the Supplier has notified the Authority of any profit warnings issued in respect of the Supplier in the three years prior to the Effective Date.

3.2 If at any time the Supplier becomes aware that a representation or warranty given by it under Clause **Error! Reference source not found.**, **Error! Reference source not found.** and/or **Error! Reference source not found.** has been breached, is untrue, or is misleading, it shall immediately notify the Authority of the relevant occurrence in sufficient detail to enable the Authority to make an accurate assessment of the situation.

3.3 In the event that the warranty given by the Supplier pursuant to Clause **Error! Reference source not found.** is materially untrue, the Authority shall be entitled to terminate the Agreement pursuant to the Call-Off clause which provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

4. Promoting Tax Compliance

4.1 All amounts stated are stated exclusive of VAT, which shall be added at the prevailing rate as applicable and paid by the Authority following delivery of a valid VAT invoice.

4.2 To the extent applicable to the Supplier, the Supplier shall at all times comply with all Laws relating to Tax and with the equivalent legal provisions of the country in which the Supplier is established.

4.3 The Supplier shall provide to the Authority the name and, as applicable, the Value Added Tax registration number, PAYE collection number and either the Corporation Tax or self-assessment reference of any agent, supplier or Subcontractor of the Supplier prior to the provision of any material Services under the Agreement by that agent, supplier or Subcontractor. Upon a request by the Authority, the Supplier shall not contract, or will cease to contract, with any agent, supplier or Subcontractor supplying Services under the Agreement.

4.4 If, at any point during the Term, there is Tax Non-Compliance, the Supplier shall:

4.4.1 notify the Authority in writing of such fact within five (5) Working Days of its occurrence; and

4.4.2 promptly provide to the Authority:

(a) details of the steps which the Supplier is taking to resolve the Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant; and

(b) such other information in relation to the Tax Non-Compliance as the Authority may reasonably require.

4.5 The Supplier shall indemnify the Authority on a continuing basis against any liability, including any interest, penalties or costs incurred, that is levied, demanded or assessed on the Authority at any time in respect of the Supplier's failure to account for or to pay any Tax relating to payments made to the Supplier under this Agreement. Any amounts due under this Clause **Error! Reference source not found.** shall be paid in cleared funds by the Supplier to the Authority not less than five (5) Working Days before the date upon which the Tax or other liability is payable by the Authority.

4.6 Upon the Authority's request, the Supplier shall provide (promptly or within such other period notified by the Authority) information which demonstrates how the Supplier complies with its Tax obligations.

4.7 If the Supplier:

4.7.1 fails to comply (or if the Authority receives information which demonstrates to it that the Supplier has failed to comply) with Clauses **Error! Reference source not found.**, **Error! Reference source not found.** and/or **Error! Reference source not found.** this may be a material breach of the Agreement;

4.7.2 fails to comply (or if the Authority receives information which demonstrates to it that the Supplier has failed to comply) with a reasonable request by the Authority that it must not contract, or must cease to contract, with any agent, supplier or Subcontractor of the Supplier as required by Clause **Error! Reference source not found.** on the grounds that the agent, supplier or Subcontractor of the Supplier is involved in Tax Non-Compliance this shall be a material breach of the Agreement; and/or

4.7.3 fails to provide details of steps being taken and mitigating factors pursuant to Clause which in the reasonable opinion of the Authority are acceptable this shall be a material breach of the Agreement;

and any such material breach shall allow the Authority to terminate the Agreement pursuant to the Call-Off Clause which provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

4.8 The Authority may internally share any information which it receives under Clauses **Error! Reference source not found.** to **Error! Reference source not found.** (inclusive) and **Error! Reference source not found.**, for the purpose of the collection and management of revenue for which the Authority is responsible.

5. Use of Off-shore Tax Structures

5.1 Subject to the principles of non-discrimination against undertakings based either in member countries of the European Union or in signatory countries of the World Trade Organisation Agreement on Government Procurement, the Supplier shall not, and shall ensure that its Connected Companies, Key Subcontractors (and their respective Connected Companies) shall not, have or put in place (unless otherwise agreed with the Authority) any arrangements involving the use of off-shore companies or other off-shore entities the main purpose, or one of the main purposes, of which is to achieve a reduction in United Kingdom Tax of any description which would otherwise be payable by it or them on or in connection with the payments made by or on behalf of the Authority under or pursuant to this Agreement or (in the case of any Key Subcontractor and its Connected Companies) United Kingdom Tax which would be payable by it or them on or in connection with payments made by or on behalf of the Supplier under or pursuant to the applicable Key Subcontract ("Prohibited Transactions"). Prohibited Transactions shall not include transactions made between the Supplier and its Connected Companies or a Key Subcontractor and its Connected Companies on terms which are at arms-length and are entered into in the ordinary course of the transacting parties' business.

5.2 The Supplier shall notify the Authority in writing (with reasonable supporting detail) of any proposal for the Supplier or any of its Connected Companies, or for a Key Subcontractor (or any of its Connected Companies), to enter into any Prohibited Transaction. The Supplier shall notify the Authority within a reasonable time to allow the Authority to consider the proposed Prohibited Transaction before it is due to be put in place.

5.3 In the event of a Prohibited Transaction being entered into in breach of Clause **Error! Reference source not found.** above, or in the event that circumstances arise which may result in such a breach, the Supplier and/or the Key Subcontractor (as applicable) shall discuss the situation with the Authority and, in order to ensure future compliance with the requirements of Clauses **Error! Reference source not found.** and **Error! Reference source not found.**, the Parties (and the Supplier shall procure that the Key Subcontractor, where applicable) shall agree (at no cost to the Authority) timely and appropriate changes to any such arrangements by the undertakings concerned, resolving the matter (if required) through the escalation process in the Agreement.

5.4 Failure by the Supplier (or a Key Subcontractor) to comply with the obligations set out in Clauses **Error! Reference source not found.** and **Error! Reference source not found.** shall allow the Authority to terminate the Agreement pursuant to the Clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause).

6 Data Protection and off-shoring

6.1 The parties agree that the Supplier shall, whether it is the Controller or Processor, in relation to any Personal Data processed in connection with its obligations under the Agreement:

6.1.1 not process or permit to be processed Personal Data outside of the United Kingdom unless the prior explicit written consent of the Authority has been obtained and the following conditions are fulfilled:

(a) the Supplier or any applicable Processor has provided appropriate safeguards in relation to any transfer of the Personal Data (whether in accordance with UK GDPR Article 46 or, where relevant, section 75 of the Data Protection Act 2018) as determined by either the Authority or the Supplier when it is the Controller;

(b) the Data Subject has enforceable rights and effective legal remedies;

(c) the Supplier or any applicable Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is processed (or, if it is not so bound, uses its best endeavours to assist either the Authority or the Supplier when it is the Controller in meeting its obligations); and

(d) the Supplier or any applicable Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

6.2 Failure by the Supplier to comply with the obligations set out in Clause **Error! Reference source not found.** shall allow the Authority to terminate the Agreement pursuant to the Clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

7 Commissioners for Revenue and Customs Act 2005 and related Legislation

7.1 The Supplier shall comply with, and shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data comply with the obligations set out in Section 18 of the Commissioners for Revenue and Customs Act 2005 ('CRCA') to maintain the confidentiality of Authority Data. Further, the Supplier acknowledges that (without prejudice to any other rights and remedies of the Authority) a breach of the aforesaid obligations may lead to a prosecution under Section 19 of CRCA.

7.2 The Supplier shall comply with, and shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data comply with the obligations set out in Section 123 of the Social Secu-

rity Administration Act 1992, which may apply to the fulfilment of some or all of the Services. The Supplier acknowledges that (without prejudice to any other rights and remedies of the Authority) a breach of the Supplier's obligations under Section 123 of the Social Security Administration Act 1992 may lead to a prosecution under that Act.

7.3 The Supplier shall regularly (not less than once every six (6) months) remind all Supplier Personnel who will have access to, or are provided with, Authority Data in writing of the obligations upon Supplier Personnel set out in Clause **Error! Reference source not found.** above. The Supplier shall monitor the compliance by Supplier Personnel with such obligations.

7.4 The Supplier shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data sign (or have previously signed) a Confidentiality Declaration, in the form provided at Annex 2. The Supplier shall provide a copy of each such signed declaration to the Authority upon demand.

7.5 In the event that the Supplier or the Supplier Personnel fail to comply with this Clause **Error! Reference source not found.**, the Authority reserves the right to terminate the Agreement with immediate effect pursuant to the clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause).

Annex 1

Excerpt from HMRC's "Test for Tax Non-Compliance"

Condition one (An in-scope entity or person)

1. There is a person or entity which is either: ("X")

   The Economic Operator or Essential Subcontractor (EOS)

   Part of the same Group of companies of EOS. An entity will be treated as within the same Group of EOS where that entities' financial statements would be required to be consolidated with those of EOS if prepared in accordance with *IFRS 10 Consolidated Financial Accounts*[1];

   Any director, shareholder or other person (P) which exercises control over EOS. 'Control' means P can secure, through holding of shares or powers under articles of association or other document that EOS's affairs are conducted in accordance with P's wishes.

Condition two (Arrangements involving evasion, abuse or tax avoidance)

2. X has been engaged in one or more of the following:

   a. Fraudulent evasion[2];

   b. Conduct caught by the General Anti-Abuse Rule[3];

   c. Conduct caught by the Halifax Abuse principle[4];

   d. Entered into arrangements caught by a DOTAS or VADR scheme[5];

   e. Conduct caught by a recognised 'anti-avoidance rule'[6] being a statutory provision which targets arrangements where either a main purpose, or an expected benefit, is to obtain a tax advantage or where the arrangement is not affected for commercial purposes. 'Targeted Anti-Avoidance Rules' (TAARs). It may be useful to confirm that the Diverted Profits Tax is a TAAR for these purposes;

[1] https://www.iasplus.com/en/standards/ifrs/ifrs10

[2] 'Fraudulent evasion' means any 'UK tax evasion offence' or 'UK tax evasion facilitation offence' as defined by section 52 of the Criminal Finances Act 2017 or a failure to prevent facilitation of tax evasion under section 45 of the same Act.

[3] "General Anti-Abuse Rule" means (a) the legislation in Part 5 of the Finance Act 2013; and (b) any future legislation introduced into Parliament to counteract tax advantages arising from abusive arrangements to avoid national insurance contributions

[4] "Halifax Abuse Principle" means the principle explained in the CJEU Case C-255/02 Halifax and others

[5] A Disclosure of Tax Avoidance Scheme (DOTAS) or VAT Disclosure Regime (VADR) scheme caught by rules which require a promoter of tax schemes to tell HM Revenue & Customs of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Section 19 and Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Section 19 and Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992.

[6] The full definition of 'Anti-avoidance rule' can be found at Paragraph 25(1) of Schedule 18 to the Finance Act 2016 and Condition 2 (a) above shall be construed accordingly.

f. Entered into an avoidance scheme identified by HMRC's published Spotlights list[7];

g. Engaged in conduct which falls under rules in other jurisdictions which are equivalent or similar to (a) to (f) above.

Condition three (Arrangements are admitted, or subject to litigation/prosecution or identified in a published list (Spotlights))

3. X's activity in *Condition 2* is, where applicable, subject to dispute and/or litigation as follows:

In respect of (a), either X:

Has accepted the terms of an offer made under a Contractual Disclosure Facility (CDF) pursuant to the Code of Practice 9 (COP9) procedure[8]; or,

Has been charged with an offence of fraudulent evasion.

In respect of (b) to (e), once X has commenced the statutory appeal process by filing a Notice of Appeal and the appeal process is ongoing including where the appeal is stayed or listed behind a lead case (either formally or informally). NB Judicial reviews are not part of the statutory appeal process and no supplier would be excluded merely because they are applying for judicial review of an HMRC or HMT decision relating to tax or national insurance.

In respect of (b) to (e), during an HMRC enquiry, if it has been agreed between HMRC and X that there is a pause with the enquiry in order to await the outcome of related litigation.

In respect of (f) this condition is satisfied without any further steps being taken.

In respect of (g) the foreign equivalent to each of the corresponding steps set out above in (i) to (iii).

E. For the avoidance of doubt, any reference in this Annex 1 to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time including any implementing or successor legislation.

[7] Targeted list of tax avoidance schemes that HMRC believes are being used to avoid paying tax due and which are listed on the Spotlight website: https://www.gov.uk/government/collections/tax-avoidance-schemes-currently-in-the-spotlight

[8] The Code of Practice 9 (COP9) is an investigation of fraud procedure, where X agrees to make a complete and accurate disclosure of all their deliberate and non-deliberate conduct that has led to irregularities in their tax affairs following which HMRC will not pursue a criminal investigation into the conduct disclosed.

Annex 2 Form

CONFIDENTIALITY DECLARATION

CONTRACT REFERENCE: [for Supplier to insert Contract reference number and contract date] ('the Agreement')

DECLARATION:

I solemnly declare that:

I am aware that the duty of confidentiality imposed by section 18 of the Commissioners for Revenue and Customs Act 2005 applies to Authority Data (as defined in the Agreement) that has been or will be provided to me in accordance with the Agreement.

I understand and acknowledge that under Section 19 of the Commissioners for Revenue and Customs Act 2005 it may be a criminal offence to disclose any Authority Data provided to me.

SIGNED:
FULL NAME:
POSITION:
COMPANY:
DATE OF SIGNATURE: