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 **10th October 2024** between the Supplier (as defined below) and the Minister for the Cabinet Office (the "**Framework Agreement**") and should be used by Buyers after making a direct award or conducting a further competition under the Framework Agreement.

The Contract, referred to throughout this Order Form, means the contract between the Supplier and the Buyer (as defined below) (entered into pursuant to the terms of the Framework Agreement) consisting of this Order Form and the Call Off Terms. The Call-Off Terms are substantially the terms set out in Annex 2 to Schedule 4 to the Framework Agreement and copies of which are available from the Crown Commercial Service website **RM6100 Technology Services 3.** The agreed Call-Off Terms for the Contract being set out as the Annex 1 to this Order Form.

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

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

This Order Form shall comprise:

1. This document headed “Order Form”;
2. Attachment 1 – Services Specification;
3. Attachment 2 – Charges and Invoicing;
4. Attachment 3 – Implementation Plan;
5. Attachment 4 – Service Levels and Service Credits;
6. Attachment 5 – Key Supplier Personnel and Key Sub-Contractors;
7. Attachment 6 – Software;
8. Attachment 7 – Financial Distress;
9. Attachment 8 - Governance
10. Attachment 9 – Schedule of Processing, Personal Data and Data Subjects;
11. Attachment 10 – Transparency Reports; and
12. 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:

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

.1.2 the Order Form;

.1.3 the Call Off Terms; and

[REDACTED]

Crown Commercial Service

.1.4 Framework Schedule 18 (Tender).

Section A
General information

Contract Details	
Contract Reference:	[REDACTED]
Contract Title:	HMCTS Crime IdAM Product Enhancement Team Managed Service
Contract Description:	Provision of a Product Enhancement Team for the delivery of the Crime Identity Management (IdAM) Managed Service.
Contract Anticipated Potential Value: this should set out the total potential value of the Contract	[REDACTED]
Estimated Year 1 Charges:	[REDACTED]
Commencement Date: this should be the date of the last signature on Section E of this Order Form	Click here to enter text.

Buyer details
Buyer organisation name The Lord Chancellor on behalf of HM Courts and Tribunal Service
Billing address Your organisation's billing address - please ensure you include a postcode HM Courts and Tribunal Service PO Box 745, Newport, Gwent, NP10 8FZ [REDACTED]
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.

Crown Commercial Service

[REDACTED]

Buyer Project Reference
Please provide the customer project reference number.
[REDACTED]

Supplier details

Supplier name
The supplier organisation name, as it appears in the Framework Agreement
CGI IT UK Limited

Supplier address
Supplier's registered address
14th Floor, 20 Fenchurch Street
London
Berkshire
EC3M 3BY

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

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

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

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

Crown Commercial Service

Guarantor Registered Address
Guarantor's registered address

Not Applicable

[REDACTED]

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	X
5.	SERVICE INTEGRATION AND MANAGEMENT	☐

[REDACTED]

Crown Commercial Service

Part B – The Services Requirement

Commencement Date
See above in Section A

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

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

Initial Term Months
24 (2 years)

Extension Period (Optional) Months
12+12+12 (1+1+1=3years)

Minimum Notice Period for exercise of Termination Without Cause (Calendar days) *Insert right (see Clause 35.1.9 of the Call-Off Terms)* 90 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:

102 Petty France, London, SW1H 9AJ

Or other site across the MoJ or HMCTS estate

Supplier Premises:

A mixture of hybrid working, with mainly home working and working from the following Sites:

14th Floor
20 Fenchurch Street
London
EC3M 3BY.

Third Party Premises:

Not Applicable

Buyer Assets
Guidance Note: see definition of Buyer Assets in Schedule 1 of the Call-Off Terms
Desk Top/Laptop where bring your own device is not applicable

[REDACTED]

Crown Commercial Service

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

- ITIL
- ISO200000 Service Management
- ISO9001 Quality Management
- ISO Information Security management Standards

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.

HTTPS://SECURITY-GUIDANCE.SERVICE.JUSTICE.GOV.UK/#CYBER-AND-TECHNICAL-SECURITY-GUIDANCE

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

See link above

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.

[REDACTED]

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

The Buyer is responsible for:

- Granting secure access to the Buyer's site.
- Provision of adequate desk space, power, telephony as required by the Supplier in order to deliver the Services.
- Access to existing knowledge articles and contracts.
- The Buyer shall not, and warrants that it shall not, provide Personal Data to the Supplier for Processing and will grant the Supplier limited, read-only access on a timebound basis to the extent required for the resolution of Incidents.

- The Buyer, as the Data Controller, remains responsible for the production of a data privacy impact assessment (DPIA) if required.
- The Supplier will be working on Buyer Systems and the Buyer remains responsible for assuring itself that the Buyer Systems provide the necessary technical and organisational measures to safeguard Personal Data and Buyer Data.
- The Buyer acknowledges that it is responsible for specifying security policies and standards appropriate to its needs, including those of its regulators, having taken into account the reputational implications of a failure of those requirements to ensure no breaches of security. No responsibility for assessing the suitability of such policies and standards passes to the Supplier on entering into this Agreement.
- The Buyer is solely responsible for undertaking a full assessment of all "Systems Safety Risks" (harm to individuals or the environment which could be associated with the use, misuse, non-use, error or failure of the Supplier's Deliverables or Services), together with planning and implementing appropriate mitigating action, and no liability for managing Systems Safety Risks, or their consequences, shall be transferred to the Supplier by entering into this Agreement or otherwise. The Buyer acknowledges that highlighting this responsibility to the Buyer fully discharges the Supplier's duty of care obligations in respect of any such Systems Safety Risks.
- The Buyer is responsible for owning the product backlog and for prioritisation of the product backlog.
- On the commencement of knowledge transfer, the Buyer is required to provide the Supplier with details of the backlog items on the agreed backlog with its incumbent supplier that have not yet been delivered. The Buyer shall, and will procure that the incumbent supplier shall, provide the Supplier with all information reasonably requested to enable the Supplier to understand all of the backlog items that are transitioning to the Supplier, including attendance at sessions to review the backlog items.
- The Buyer is responsible for the performance of third parties engaged by it that the Supplier requires access to and where a Buyer third party causes an Incident and resolution of such Incident is outside of the Supplier's control, the Supplier shall not be deemed to be in Default or to have committed a Service Level Failure.
- The Buyer is responsible for licence management and third-party licences required by it to access or make use of the Supplier's solution including, for the avoidance of doubt,

third party licences relating to ForgeRock and for procuring any additional or 4th line support required from ForgeRock.

- The Buyer shall ensure suitable Buyer and incumbent supplier representatives are available to undertake the knowledge transfer and transition activities in accordance with the Outline Implementation Plan and shall, and will procure that the incumbent supplier shall, provide all information reasonably requested by the Supplier to enable it to complete knowledge transfer and transition activities.

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	X
Part B – Long Form Governance Schedule	☐

The Part selected above shall apply this Contract.

Change Control Procedure – Option Part A or Part B

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

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

- for the purpose of Paragraph 3.1.2 (a), the figure shall be £[*insert details*]; and
- for the purpose of Paragraph 8.2.2, the figure shall be £[*insert details*].

[REDACTED]

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	X
S2: Testing Procedures	X
S3: Security Requirements (either Part A or Part B)	Part A X or Part B ☐
S4: Staff Transfer	X
S5: Benchmarking	X
S6: Business Continuity and Disaster Recovery	X
S7: Continuous Improvement	X
S8: Guarantee – Not Used	☐
S9: MOD Terms – Not Used	☐

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

Additional Clauses	Tick as applicable
C1: Relevant Convictions	X
C2: Security Measures	X
C3: Collaboration Agreement – Not Used	☐

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

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

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.

There will be no Staff Transfer on commencement.

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.

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.

Crown Commercial Service

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.*

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

Crown Commercial Service

Section E
Contract Award

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

SIGNATURES

For and on behalf of the Supplier

Name	[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

Note: During contract engrossment, the Parties have agreed that the core Services will no longer be delivered in accordance with a SOW model, but on a fixed capacity basis with an associated fixed monthly Service Charge. SOWs may be used for additional capacity requirements or change work. The Parties have also agreed to vary the standard hours and on-call hours to align with other related services, such that the standard and on-call hours in Attachment 4 of this Order Form will apply to the Services.

1 DEFINITIONS

Table 1

Expression or Acronym	Definition
AMS	**Application Management Service**
CPS	**Crown Prosecution Service**
HMCTS	**HM Courts and Tribunal Service**
HMCTS DTS	**HM Courts and Tribunal Service Digital & Technology Services**
HMPPS	**HM Prison and Probation Service**
IdAM	**Identity Management**
KC's	**King's Counsel**
MoJ	**Ministry of Justice**
PET	**Product Enhancement Team**

2 SCOPE OF REQUIREMENT

The Scope of the Services the Potential Provider shall provide is a PET as a Managed Service to manage (including third line incident management and resolution) the Crime IdAM system combined with 3rd line support.

The Potential Provider shall provide Services to maintain the Crime IdAM system through a PET using personnel of requisite skill, experience, expertise, and qualifications.

2.1 The Potential Provider shall provide:

- Product Enhancement Capability – Development of the Crime IdAM service to meet the arising (functional and non-functional) needs of the business; this includes capacity planning as the number of services (and users) increase.
- Product Maintenance Capability – The re-alignment of the Crime IdAM service with the latest upgrades and patches available for the underlying technologies
- Third line support as per the requirement set out in 4.7 Secondary Function.
- Release management – the scheduling management and delivery of regular software releases to the production environment
- Assistance to other teams

2.2 The Potential Provider is responsible for managing the PET. The Potential Provider's appointed delivery manager will act as the Potential Provider Representative, and shall manage the PET, assure quality of deliverables, reporting and those agreed outcomes are met in line within agreed timescales.

Crown Commercial Service

2.3 Out of Scope

- The following activities are out of the scope of this service requirement:
  - 1st and 2nd Line Support
  - Hosting
- Common Platform, Rota and any other applications accessible via Crime IdAM.

The Potential Provider will not be responsible for the hosting of any of the services.

3 THE REQUIREMENT

3.1 Requirements

3.1.1 The development team must manage and maintain a Product Enhancement function / continuing development combined with third line production support when needed.

3.1.2 Scope of delivery will include a backlog, consisting of known issues, technical debt, improvements, and evolving requirements. Evolving requirements may include extension and adaptation of the service to improve certain elements of the existing functionality, as well as new functionality, to improve the service offered by the product to the business.

3.1.3 HMCTS DTS will provide 1st and 2nd line support. The MSP will only be required for 3rd line support. Should an issue need to be raised with 3rd line support, a ticket will be assigned to them on HMCTS Service Now, and/or the HMCTS Product Manager will liaise with the MSP directly.

3.1.4 The main 3rd party suppliers that will be liaising with the HMCTS Crime IdAM PET will be the Common Platform Technical Teams, the Magistrates Rota Technical Team and the CaTH Technical Team. HMCTS requires the Potential Provider to co-operate with any other service provider notified by the Buyer from time to time.

3.1.5 The Potential Provider will be responsible for maintaining a suitably skilled resource pool that will enable them to scale up and scale down the PET staffing/resource.

3.1.6 Updates and enhancements shall be delivered using Agile methodology and Sprints (typical duration of 2 weeks). Sprints will be agreed between the parties and documented.

4.1.7 Knowledge Transfer Period: Following the signing of the contract, the Potential Provider's team will initially be required to work onsite at the Primary/Secondary location during the knowledge transfer period for a period of 9 weeks working a fulltime, five-day week.

3.2 Primary Function

3.2.1 The primary function of the Product Enhancement Team ('PET') is to develop and implement business and technical enhancements to the Crime IdAM system i.e. updating current functionality, implementing new functionality ('Enhancements') or updating existing technologies.

3.2.2 **Product Enhancements – Functional Requirements**

3.2.3 **Table 2**

#	Objective/Requirement	MoS-CoW
1A	**Provide third line support to users and Application Management Service (AMS) in live production.** **Third Line support constitutes:** **1. Investigating and identifying solutions to issues found in the live service as received from 2nd Line support and as detailed in a Jira/ServiceNow ticket.**	**Must**

[REDACTED]

#	Objective/Requirement	MoS-CoW
	2. Supporting the Application Management Service team to resolve, trouble shoot and prioritise issues reported by the Buyer's users, and captured in ServiceNow, in the live production environment. 3. All new issues will be logged on Jira and ServiceNow or otherwise, where applicable, existing tickets updated. 4. Reporting to be carried out monthly.	
B	Provide support to the AMS team for releases to pre-production and production. Log and report as above where applicable.	Must
C	Upgrade to the latest revision of the various technologies that comprise Crime IdAM.	Must
D	Apply user interface enhancements to the various Crime IdAM front-end applications.	Must
E	Implement security changes highlighted in the ITHC report(s); apply security upgrades and implement security enhancements.	Must
F	Resolution of existing "Known Issues" that have been previously identified, and a subsequent Jira/ServiceNow ticket created and added to the Crime IdAM backlog, or additional problem tickets or issues/defects that will be identified by users of the live Crime IdAM service. All issues are to be resolved to the satisfaction of the Business Product Owner and acceptance criteria met. Report on assigned tickets on a two-week cycle or otherwise per sprint basis.	Must
G	Provision of the improvements that have been (or will be) identified in the area of "Technical Debt". For the purposes of this Call-off Contract, Technical Debt shall be defined as: 'Technical debt is a concept that reflects the implied cost of additional rework caused by choosing an easy solution now instead of using a better approach that would take longer.' Technical Debt stories are therefore those Stories required to rework current functionality which, whilst working, is either limited or otherwise limits further application development. Monitor, log and report	Must
2.	Estimation of the effort required to deliver the prioritised Product Backlog and reflect this in an incremental release plan that will allow early delivery of critical functionality. Participate in the analysis, refinement, assessment and implementation of functional enhancements, as identified through user research and feedback providing technical input and recommendation as to any potential solution and development timescales.	Must
3.	Ensure that all documentation currently stored in the Confluence document repository is up to date where either; Potential Provider Personnel delivery of services makes a change that causes existing documentation to become inaccurate, or in the event that new documentation is required.	Must

#	Objective/Requirement	MoS-CoW
4.	Maintenance of the HLSA, service transition collateral and knowledge transfer to 2nd line business support team. Provide knowledge transfer documentation and sessions as and when required to ensure continuity of service. The primary knowledge transfer vector shall be the production or updating of project documentation including code annotation, wiki's, FAQ's or similar. Potential Provider Personnel may be required to hold knowledge transfer workshops to contextualise project documentation.	Must
5.	Provide knowledge transfer to MoJ staff or a new Potential Provider; document sessions as and when required to ensure continuity and transition of service. The primary knowledge transfer vector shall be the production or updating of project documentation including code annotation, wiki's, FAQ's or similar. Potential Provider Personnel may be required to hold knowledge transfer workshops to contextualise project documentation.	Must
6.	Assist in the provisioning of a Crime IDAM stack plus associated support of the BAE (PR) environment. - Support the creation, setup and configuration of resource within BAE to stand up a full Crime IDAM instance for BAE users. This will be built in addition to the existing instances (SIT, NFT, PRP, PRD). - Ongoing support for infrastructure components and services in BAE. - Deploying/updating the BAE environment with new releases in accordance to the cadence/timings agreed with the business.	Must
7	Accurate and timely reporting of the Service Line Measures within the monthly account and service review.	Must
8	The Potential Provider will work with the Buyer to review the reported Service Line Measures within the monthly account and service review	Must

3.3 Deliverables in Detail

3.3.1 **Table 3 – Core Deliverables and Acceptance**

#	Epics	Acceptance Criteria	Accepted By
	The work below covers the epic level work that is currently ready for prioritisation in the Crime IdAM backlog and will be considered as areas to be worked on for future releases (Product owner will decide the priority). Sprints will include the following, but are subject to change as deemed appropriate by the Product Owner:		
1	Integrating CaTH with Crime IdAM	The Definition of Done	Business Product Owner or delegate ('BPO')
2	Remove the Live Sync from IDM	The Definition of Done	BPO

#	Epics	Acceptance Criteria	Accepted By
3	Proof of concept using Kubernetes in the release pipeline	The Definition of Done	BPO
4	Moving to continual release and using feature flags for releasing work into production	The Definition of Done	BPO
5	Improving data integrity	The Definition of Done	BPO
6	Introducing an esendex stub	The Definition of Done	BPO
7	Improving automated testing throughout the Crime IdAM components	The Definition of Done	BPO
8	Custom Health Dashboard for ForgeRock components using DynaTrace	The Definition of Done	BPO
9	Improve the speed loading users onto the system	The Definition of Done	BPO
10	Profile ISG and dataloader with dataloader running	The Definition of Done	BPO

3.4 Working Practices (Potential Provider Obligations)

3.4.1 **Table 4**

#	Working Practices	MoSCoW
1	Work as part of a multi-disciplinary, self-organising team, using Agile principles and methodologies. Full participation in the Agile processes of the team including attendance at team stand-ups, planning sessions and other Agile ceremonies.	Must
2	Maintain and encourage high standards of practice. Apply Agile principles and methodologies in a way which aligns with the values and goals of the business and the wider programme. Resources will be expected to work to the core values and standards as set out within the Civil Service conduct and guidance https://www.gov.uk/government/collections/civil-service-conduct-and-guidance;	Must
3	Collaborate with the Buyer's service project and architecture team personnel e.g. Designers, Solution Architects, BA's, Business Architects, and the development / other Buyer teams;	Must
4	Keep a user focused mind-set and consider the impact of their work on the user's experience and the wider business and programme.	Must
5	Ensure knowledge transfer within the Buyer's programme.	Must
6	The Potential Provider shall engage with the relevant HMCTS/DTS Teams to observe and help improve practice standards.	Must
7	The Potential Provider shall attend the following Governance forums: • Scrum ceremonies • Progress Reporting	Must

	• **Commercial review meetings** • **Stakeholder Demonstrations**	
8	**Core working hours are between the hours of 8:00 to 18:00, Monday to Friday. Any work to be undertaken outside of the core working hours must be given written approval. These costs are to be Travel &Subsistence inclusive.**	**Must**
9	**Sprint reports are correct and delivered within 3 working days of the end of the reporting period.** **The 'Sprint' Report must contain, as a minimum, the following information:** ▪ **Sprint Summary** ▪ **Sprint Overview of what was achieved during the Sprint** ▪ **Reason for any deviation from what was expected verses what was achieved** ▪ **Information regarding any Releases delivered during the Sprint** ▪ **Details of stories signed off in the Sprint** ▪ **Details of any additional stories brought into the Sprint** ▪ **Details of any stories carried forward into the Sprint** ▪ **Details of any stories being carried forward to the next Sprint** ▪ **Burndown chart** ▪ **Any Risks, Issues and Dependencies** **Other agreed reports are correct and delivered within 5 working days of reporting period.**	**Must**

3.5 Core Skills for Potential Provider Resources

3.5.1 The Potential Provider team must be appropriately skilled as to be able to deliver the following to best development and related industry practice.

3.5.2 **Table 5**

#	Core Skill	MoSCoW
1	**Effective in working in multi-discipline environments focused on meeting user needs using agile methodologies and delivering digital improvement outcomes**	**Must**
2	**High level expertise in supporting the ForgeRock product stack**	**Must**
3	**High level expertise of agile testing strategies and automation**	**Must**
4	**High level expertise in a security testing and delivery cycle**	**Must**
5	**High level expertise working with multiple cloud vendor technologies and tools (e.g Azure)**	**Must**
6	**High level expertise with usable Crime IdAM solutions including integrating them in live services.**	**Must**
7	**High level expertise in Development with:** • **front-end coding (HTML5, CSS 3, Angular 2, Javascript); and** • **back-end coding (SQL, Java 8, DropWizard, JMS).**	**Must**
8	**High level expertise operating DevOps and continuous delivery principles, in live national scale operations. Reference practices**	**Must**

#	Core Skill	MoSCoW
	that enable safe, sustainable releases into live production, mitigating risk to existing operations	
9	**High level expertise in delivering as part of a live operational service**	**Must**
10	**High level expertise delivery using configuration management, orchestration and monitoring tooling (Encryption & Hardening, Sonarqube, OWASP, Reverse Proxies, Ansible, Zabbix, ELK stack).**	**Must**
11	**High level expertise Effective user centric design, personal data, digital transactions, security, and privacy;**	**Must**
12	**Effective use of digital test tools and technologies necessary for development of test artefacts. These include but are not limited to:** • **Test tools such as JMeter, Junit, Selenium, WebDriver, Protactor, ZAProxy or RestEasy, BURP, Pa11y.** **Good technical understanding of:** • **Java** • **NodeJS** • **HTML / SCSS** • **Gulp / Webpack** • **Jenkins** • **Git/Gerrit** • **Dynatrace** • **Ubuntu** • **Maven** • **Docker** • **Tomcat** • **Nginx** • **Linux (Redhat)** • **JIRA/Confluence** • **Groovy** • **Azure** • **VM Templates** • **Networks** • **PostgreSQL** • **ForgeRock AM, IDM, IG, DS including LDAP** • **ActivityMQ** • **HAPROXY**	**Must**
13	**Production of high-quality documentation. Documentation may include but is not limited to:** ▪ **Presentations and briefings** ▪ **Test cases**	**Must**

[REDACTED]

#	Core Skill	MoSCoW
	▪ Test scripts ▪ Test reports ▪ Test Metrics	
14	Effective stakeholder management including but not limited to working transparently and collaboratively with governance and decision-making stakeholders.	Must

Non-Functional Requirements
4.5.3 Table 6

Service Grouping	Requirement	MoSCoW
General Service Management	The service provider to operate a governance structure that reflects the Buyer's governance structure with appropriate management escalation points.	Must
General Service Management	The service provider to provide support, as defined and agreed between both parties, to maintain their Service Management Policies, Processes and Procedures. The service provider to adopt any changes made to the HMCTS Service Management Policies, Processes and Procedures throughout the Call-Off Contract Period that are agreed through the Governance Framework.	Must
Major Incident Management	The service provider to provide progress updates on P1 and P2 major incidents to the HMCTS major incident management function according to DTS default service level agreement.	Must
Release Management	The service provider will go through onboarding into the release management function in line with the HMCTS release management process.	Must
Release Management	The service provider is to provide detailed release plan(s).	Must
Disaster Recovery	The service provider to develop, maintain and provide an up-to-date Disaster Recovery Plan, developed in line with ISO27031 standard and to be tested at least annually. The service provider to review/update the DR plan following live/test invocations and or significant changes to the functionality of the service.	Must
Service Continuity	The service provider to proactively monitor the service, identifying risks and proposing remediation actions that may impact on the continuity of service.	Must
Service Measurement and Performance	Data and reporting for the services for the agreed period, to include performance against availability % of actual and expected targets, and in line with the HMCTS information and data standards.	Must

[REDACTED]

Management		
Service Level Management	**The service provider to measure suitable incident, problem and change process aligned to the HMCTS incident process, for the agreed reporting period and in line with the HMCTS information and data standards and the service levels agreed with the service provider.**	**Must**
Data Migration	**The service provider to facilitate data migration from the Buyer's existing, and the future choice of solution. In conjunction with Buyer agreement and DASI.**	**Must**
Collaboration	**The service provider to co-operate with any other service provider notified to them by the Buyer from time to time providing: (i) reasonable information (including any documentation) (ii) advice; and (iii) reasonable assistance (in connection with the services procured) to any such other service provider to enable them to create and maintain technical or organisational interfaces. To support design, delivery and integration of processes and services from multiple service providers to deliver end-to-end services. On the expiry or termination of this contract for any reason, to enable the timely transition of the services (or any of them) to the Buyer and/or to any replacement service provider in accordance with the following collaborative working principles: (A) proactively leading on, mitigating and contributing to the resolution of problems, defects or issues irrespective of its contractual obligations, acting in accordance with the principle of "fix first, settle later"; (B) being open, transparent and responsive in sharing relevant and accurate information with such other service providers; (C) where reasonable, adopting common working practices, terminology, standards and technology and a collaborative approach to service development and resourcing with such other service providers; (D) providing reasonable cooperation, support, information and assistance to such other service providers in a proactive, transparent and open way and in a spirit of trust and mutual confidence; and (E) identifying, implementing and capitalising on opportunities to improve deliverables and deliver better solutions and performance throughout the relationship cycle.**	**Must**
Collaboration	**The service provider to work with the Buyer and other service providers in the development, implementation**	**Must**

[REDACTED]

	and operation of inter-supplier governance processes and meeting structures.	
Collaboration	**The service provider to willingly engage and work with all relevant HMCTS teams to develop, test and implement the required solution.**	**Must**
Collaboration	**The service provider to escalate any issues with other service providers, where they feel they are unable to resolve without intervention from the Buyer and/or other service providers in the Buyer's operating environment.**	**Must**
Supplier Management	**The service provider will facilitate a recurring monthly service review meeting and will present the service performance report. The report should be ready and sent for review at least 5 working days before the monthly service review meeting.**	**Should**
Risk Management	**The service provider to have a risk management strategy, risk register and align with HMCTS' DTS risk management process**	**Must**

Security Non-Functional Requirements
Table 7

Service Grouping	**Requirement**	**MoSCoW**
Operations Security	**The solution must ensure security log events and audit events are retained and available for a configurable period of time. At a minimum, the solution must ensure security events and audit events (1) are stored and made available for 90 days (2) contain an accurate date and time stamp (3) are verbose enough to support effective security incident management and forensics.**	**Must**
Access Control	**The solution must implement secure authentication and authorisation mechanisms to reduce the likelihood of unauthorised access to the solution. At a minimum, the solution must support OAuth 2.0, OIDC, SAML2.0 and LDAPS (or equivalent).**	**Must**
Access Control	**The solution must support or implement Multi-Factor Authentication (MFA). At a minimum, Time-based One-Time Password (TOTP) must be supported.**	**Must**
Access Control	**The solution must support user authentication to existing Identity and Access Management (Crime IdAM) services used by HMCTS. At a minimum, the solution must (1) support Microsoft Entra ID (formerly Azure Active Directory) (2) respond to changes to user accounts or permissions within the HMCTS Crime IdAM, within the minimum time possible (maximum 30 minutes).**	**Must**

Access Control	**The solution must support Single Sign-On (SSO)**	**Must**
Access Control	**The solution must provide the technical capability to configure a robust and granular Role Based Access Control (RBAC) model. At a minimum, the solution must provide the ability to (1) manage user permissions at an individual, team and group level (2) support Just-in-Time (JIT) access (3) enforce the Principle of Least Privilege (PoLP) (4) separate the request and approval stages of account creation (5) log changes to user permissions.**	**Must**
Information Security Aspects of Business Continuity Management	**The supplier must develop and maintain a Business Continuity and Disaster Recovery Plan that meets the requirements of ISO/IEC22301 (https://www.iso.org/standard/75106.html).**	**Must**
Operations Security	**The supplier must ensure any changes to hardware and software configurations are performed under formal change control. At a minimum, the supplier must audit against unauthorised changes at least once during any period of twelve months and provide evidence to HMCTS of audit findings.**	**Must**
Supplier Relationships	**The supplier must ensure, and provide evidence to HMCTS, that all security requirements – functional and non-functional – applicable to the solution or service, will flow down in the supply chain and will apply to all sub-contractors, partners, and suppliers that participate in the solution or service.**	**Must**
Cryptography	**The solution must provide a secure mechanism to store and retrieve credentials, cryptographic keys and secrets based on NCSC guidance (https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/choosing-and-configuring-a-kms-for-secure-key-management-in-the-cloud). At a minimum, the solution must (1) use a tamper-resistant secure storage (2) provide a mechanism for automated rotation of keys and secrets (3) provide a mechanism for deletion or revocation of cryptographic keys (4) log and monitor access to cryptographic keys.**	**Must**
Compliance	**The supplier must hold and maintain Cyber Essentials (CE) Plus certification the scope of which includes the systems within the solution provided to HMCTS.**	**Must**
Asset Management	**The supplier must implement measures to secure the physical handling, use, storage, transport and disposal of HMCTS information assets (whether in paper or electronic form) in accordance with the Government Security Classification Policy (https://www.gov.uk/government/publications/government-security-classifications) and SMP.**	**Must**

Compliance	**The solution must ensure all HMCTS data is stored, supported and processed within the United Kingdom (UK). The HMCTS SIRO must approve any departure from this.**	**Must**
Compliance	**The supplier must ensure that all aspects of the service provided to HMCTS is performed in accordance with Data Protection Legislation (UK GDPR and UK DPA), comply with both the law and good practice, respect the rights of individuals, be open and honest about how it handles personal data.**	**Must**
Asset Management	**The supplier must decommission, dispose, sanitise or destruct infrastructure and data in accordance with National Cyber Security Centre (NCSC) guidance (https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media). The supplier must provide a decommissioning approach document, at least 3 months ahead of the first planned decommissioning activity, detailing the decommissioning and disposal methodology for approval by HMCTS.**	**Must**
Compliance	**The supplier must comply with HMCTS Detailed Security Requirements provided with the contract.**	**Must**
Cryptography	**The solution must implement cryptographic controls to provide data at rest protection for all HMCTS information assets based on NCSC guidance (https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-2-asset-protection-and-resilience#principle23). At a minimum, the solution must (1) not use NIST deprecated or disallowed ciphers (2) support symmetric algorithm AES (3) support 256-bit key length (4) support AES-GCM or AES-XTS modes of operation (5) support SHA-256 hashing algorithm.**	**Must**
Cryptography	**The solution must implement cryptographic controls to provide data in transit protection for all HMCTS information assets based on NCSC guidance (https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data). At a minimum, the solution must (1) not use NIST deprecated ciphers (2) support TLS 1.2 (3) disable TLS features known to be insecure (4) support 2048-bit RSA or ECDSA-256 P-256 Curve signing algorithms (5) support SHA-256 hashing algorithm.**	**Must**
Operations Security	**The supplier must ensure devices used to access or manage HMCTS data under the management authority of the supplier have a minimum set of security policy configurations enforced. At a minimum, all supplier devices must satisfy the security requirements set out in the NCSC Device Security guidance (https://www.ncsc.gov.uk/collection/device-security-guidance).**	**Must**

Operations Security	**The solution must enforce physical or logical segregation between production and non-production environments.**	**Must**
Compliance	**The supplier must allow for audits and inspections of its data processing activity by HMCTS or an auditor designated by HMCTS.**	**Must**
Compliance	**The supplier should conduct internal security audits from time to time (and at least annually) across the scope of the ISMS and additionally after any change or amendment to the ISMS or SMP. At a minimum, security audit findings should be shared with HMCTS in the form of a report.**	**Should**
Asset Management	**The supplier must produce and maintain an accurate inventory of information, system, hardware (where applicable) and software assets used to deliver the service.**	**Must**
Compliance	**The supplier must hold and maintain valid ISO 27001 certification for their Information Security Management System (ISMS). The certification must be issued by a UKAS registered certification body the scope of which fully and explicitly includes the system(s) used for the solution, service and data and all related operations and procedures.**	**Must**
Access Control	**1. The solution must ensure that user accounts for self-service users meet the following requirements:** **a. Joiner's user accounts are automatically created once the person/appointment record meets given criteria.** **b. User accounts are automatically updated as appropriate when staff transition between teams.** **c. User accounts remain active for 90 days after the individual's leaving date as recorded on the person record and are automatically deactivated after the 90-day period.**	**Must**
Access Control	**2. The solution must ensure that user accounts for System Administrator & Operational users meet the following requirements:** **a. Joiner's user accounts are validated and enabled by a system administrator.** **b. Accounts for users transitioning between teams are subject to validation and enablement/disablement by a system administrator.** **c. User accounts are automatically deactivated for staff who leave the organisation.**	**Must**
Human Resource Security	**The supplier must ensure all personnel (and those within the supply chain) are based in the United Kingdom (UK). The HMCTS SIRO must approve any departure from this.**	**Must**
Operations Security	**The solution must implement malware controls to detect and prevent malware-based attacks. At a minimum, the**	**Must**

	solution must (1) use up-to-date malware detection signatures or heuristics (2) prevent attacks in near real-time (3) be monitored to ensure malware controls are always enabled (4) meet NCSC pattern for Safely Importing Data (https://www.ncsc.gov.uk/guidance/pattern-safely-importing-data) for any function designed to ingest, upload or store data from an untrusted source.	
System Acquisition, Development, and Maintenance	**The supplier should share security related information about the solution to assist HMCTS in completing the NCSC Cyber Assessment Framework (CAF)(https://www.ncsc.gov.uk/collection/caf)**	**Should**
System Acquisition, Development, and Maintenance	**The solution must meet all applicable requirements of the NCSC Cloud Security Principles (https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles). At a minimum, all multi-tenant cloud services must demonstrate how tenant separation or boundaries are implemented within compute, storage and data flows and networking.**	**Must**
System Acquisition, Development, and Maintenance	**The solution must demonstrate implementation of the NCSC Secure Design Principles (https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles).**	**Must**
Communications Security	**The solution must implement network security controls to make a network compromise difficult or reduce the impact of any network-based attack. At a minimum, controls should include (1) limiting all inbound and outbound traffic to only those sources/destinations and protocols required for the solution to function (2) network segmentation or zones (3) preventing lateral movement based on NCSC Preventing Lateral Movement Guidance (https://www.ncsc.gov.uk/guidance/preventing-lateral-movement) (4) preventing Denial-of-Service (DoS) attacks.**	**Must**
System Acquisition, Development, and Maintenance	**The solution must ensure any web applications and APIs are designed and implemented to prevent common security attacks such as those listed in the OWASP Top 10 (https://owasp.org/www-project-top-ten/).**	**Must**
Physical and Environmental Security	**The supplier must implement physical security controls at locations used in the provision of the solution and service. At a minimum, National Protective Security Authority (NPSA) guidance (https://www.npsa.gov.uk/advice-guidance) must be consulted to identify proportionate controls for preventing unauthorised physical access,**	**Must**

	damage and interference to information processing facilities where HMCTS data may be stored, processed and managed from.	
Information Security Policies	**The solution should comply with applicable HMCTS Security Policies (https://tools.hmcts.net/confluence/display/ISMS/Policy+Areas).**	**Should**
Information Security Policies	**The supplier should comply with applicable HMCTS Security Policies (https://tools.hmcts.net/confluence/display/ISMS/Policy+Areas)**	**Should**
Access Control	**The supplier must ensure segregation of duties by privileged users of the services. At a minimum this must include (1) ensuring the Principle of Least Privilege (PoLP) is always applied (2) ensuring separation of request and approval for account creation (3) logging changes to user permissions (4) regularly reviewing privileged user access.**	**Must**
Information Security Incident Management	**The supplier and HMCTS must notify the other upon becoming aware of any security incident, breach of security or any potential or attempted breach of security (including throughout the supply chain) in accordance with the ISMS, SMP and HMCTS Security Incident Management Policy. (https://tools.hmcts.net/confluence/display/ISMS/Security+Incident+Management).**	**Must**
System Acquisition, Development, and Maintenance	**The supplier must produce and maintain an information security risk assessment of the solution based on a formal risk assessment methodology and share the output with HMCTS in the form of a documented information security risk register. At a minimum the risk assessment must include (1) risk events (2) risk causes (3) risk impact (4) risk severity (5) mitigating controls**	**Must**
Compliance	**The supplier must ensure that all changes to services impacting IT security are approved in accordance with the agreed change procedure and take account of the latest Security Aspects Letter (SAL)(https://tools.hmcts.net/confluence/display/ISMS/SAL+Template).**	**Must**
System Acquisition, Development, and Maintenance	**The solution components must be deployed and configured in accordance with any published and applicable secure deployment or configuration guides made available by Vendors, NCSC or Center for Internet Security (CIS). For example:**	**Must**

	Microsoft Cloud Security Benchmark (https://learn.microsoft.com/en-us/security/benchmark/azure/) AWS Security Documentation (https://docs.aws.amazon.com/security/) NCSC Device Security Guidance for Windows (https://www.ncsc.gov.uk/collection/device-security-guidance/platform-guides/windows) CIS Benchmark for RHEL (https://www.cisecurity.org/benchmark/red_hat_linux)	
Operations Security	**The supplier must ensure the solution is under 24x7x365 security monitoring to detect suspicious and unauthorised activities based on NCSC Security Monitoring guidance (https://www.ncsc.gov.uk/files/NCSC_SOC_Feeds.pdf)**	**Must**
Operations Security	**The supplier should provide an automated mechanism to export security event logs to HMCTS security monitoring systems.**	**Should**
Compliance	**The supplier must prepare, develop, maintain and deliver HMCTS for approval a complete and up to date Security Management Plan (SMP) covering all services delivered under contract. At a minimum, the SMP must (1) be structured in accordance with the HMCTS SMP template (https://tools.hmcts.net/confluence/display/ISMS/SMP+Template) (2) identify how the supplier's ISMS applies to the services offered to HMCTS (3) explicitly detail how security non-functional requirements and outcomes are being implemented or met (4) identify the necessary delegated organisational roles defined for those responsible for delivering and overseeing the SMP (5) detail the supplier approach and processes for delivering the services using Sub-Contractors and third parties authorised by HMCTS.**	**Must**
Organisation of Information Security	**The supplier must provide HMCTS with a Single Point Of Contact (SPOC) to act as coordinator and focal point for all the security aspects to the service and the SPOC (or a delegate) must be available to attend regular security working group meetings with HMCTS.**	**Must**
Operations Security	**The supplier must not extract/export any HMCTS data outside of the service, without written consent from HMCTS. Any HMCTS approved extract/export must be strictly controlled and recorded.**	**Must**
Operations Security	**The supplier should comply with any Security Operating Procedures (SyOPs) that have been issued to HMCTS by organisations for which HMCTS processes data. At a**	**Should**

	minimum, this will include SyOPs from (1) Home Office (2) MoJ (3) Judiciary	
System Acquisition, Development, and Maintenance	**The solution must ensure any system-to-system data flows or Application Programming Interfaces (APIs) are protected using good practice security controls. At a minimum, controls should include (1) authentication (2) integrity checking (3) encryption (4) limited data exposure (5) ensuring all third-party interfaces are covered by any MoU or other type of agreement.**	**Must**
System Acquisition, Development, and Maintenance	**The solution technical design documents issued to HMCTS must explicitly detail how HMCTS technical security non-functional requirements and outcomes are being implemented or met. At a minimum, all technical design documents must (1) include a dedicated security section (2) highlight any shortcomings against HMCTS technical security non-functional requirements (3) highlight any single point of failure that could impact the availability of the solution.**	**Must**
Operations Security	**The supplier must perform regular vulnerability scanning of all the components within the solution. At a minimum, the scope must include (1) devices (2) infrastructure (3) software (4) firmware (5) software dependencies (6) application code analysis (SAST and DAST).**	**Must**
Operations Security	**The supplier must remediate all vulnerabilities in accordance with the HMCTS Vulnerability Management Policy (https://tools.hmcts.net/confluence/display/ISMS/Vulnerability+Management). At a minimum, CRITICAL severity vulnerabilities must be remediated as soon as reasonably practical (take first priority) and HIGH severity vulnerabilities remediated within 7 days.**	**Must**
Operations Security	**The supplier should provide regular reporting on vulnerability management. At a minimum, this must include information relating to (1) vulnerabilities detected (2) exploitability (3) mitigating controls (4) recommendations for remediation (4) remediation progress.**	**Should**
Compliance	**The supplier must perform an IT Health Check (ITHC) of the solution under the CHECK scheme (https://www.ncsc.gov.uk/information/check-penetration-testing). At a minimum, this must include (1) performing an ITHC within the last six months of service commencement, thereafter annually and upon significant change to the system (or a system component) (2) a scope that contains all components within the solution or a subset that has been approved by HMCTS (3) sharing ITHC report findings with HMCTS (4) remediation of all discov-**	**Must**

	ered vulnerabilities in accordance with the HMCTS Vulnerability Policy (https://tools.hmcts.net/confluence/display/ISMS/Vulnerability+Management)	
System Acquisition, Development, and Maintenance	**The solution must ensure live HMCTS data (or copies of) are only stored in production (operational) systems.**	**Must**
Information Security Aspects of Business Continuity Management	**The supplier must test backup solutions. At a minimum this must include (1) a backup test at least every three months (2) verifying data reliability and integrity of data in scope of the ISMS (3) ensuring that any testing meets the requirements of the BCDR plan (4) verifying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) can be met.**	**Must**
Human Resource Security	**The supplier must ensure that all supplier and sub-contractor staff who have access to personal data, including staff in their supply chain if appropriate, undergo a session of data protection and information risk awareness training on induction and annually thereafter.**	**Must**
Operations Security	**The supplier must ensure all software and hardware is supported by a vendor that produces regular security updates. At a minimum, the supplier must (1) inform HMCTS six months in advance of software or hardware reaching end of vendor support (2) inform HMCTS if extended support agreements have been purchased to obtain security updates.**	**Must**
Human Resource Security	**The supplier must perform appropriate checks on all personnel involved in the design, delivery and operation of the solution (pre-employment, during employment, termination and change of employment) in order to ensure the security of HMCTS information assets and the safety of staff and individuals within HMCTS. At a minimum, personnel must successfully complete Baseline Personnel Security Standard (BPSS)(or equivalent) pre-employment screening before being granted access to HMCTS information assets (https://www.gov.uk/government/publications/government-baseline-personnel-security-standard).**	**Must**
Human Resource Security	**The supplier must ensure all personnel (and those within the supply chain) hold the relevant vetting and clearance in accordance with the HMCTS Vetting and Clearance Policy (https://tools.hmcts.net/confluence/display/ISMS/Vetting+and+Clearance). The HMCTS SIRO must approve any departure from this. At a minimum, all personnel with access to (1) bulk personal data or admin-**	**Must**

	istrative privileges will require Security Check (SC) clearance (2) Home Office or Policing systems will require Non-Police Personnel Vetting (NPPV) Clearance.	

3.6 Change

3.6.1 **Change of Provider Personnel**

a) The Potential Provider shall deploy replacement resource within 10 working days. In like for like replacement of an existing resource, Potential Provider shall ensure that there is no break in service and that the incoming resource receives an adequate handover from the outgoing resource. The Potential Provider must ensure that such handover includes an overlap of time on site to ensure proper transition, such overlap to be 2 weeks or otherwise as mutually agreed by the parties where required.

b) The Potential Provider shall exit a resource due to gross misconduct within 0 working days.

c) The Potential Provider shall not remove or swap-out personnel from the service teams without providing 10 days' notice each in case and ensuring adequate handover as above.

Notwithstanding the above, Supplier shall not remove any key personnel as identified from time to time, insofar as such removal is within the Supplier's control, without Buyer's permission.

d) Changes include but are not limited to:

- Variation to the mix of roles provided.
- Variation to the capacity of the team

e) The Parties acknowledge that a core objective of the Service is business transformation and accordingly that the configuration of the teams may vary substantially over the term of the engagement as the parties agree and implement transformation targets. Such variation may, by agreement, alter the nature of the roles and the assignment of responsibilities assigned to each role as documented in this Invitation To Tender.

4.6.3 Change Management

Changes to any element of the Backlog, sprint planning, pre-release work, fixes, improvements or how the service is to be delivered under this Call-off contract shall be proposed via the Buyer's Change Management Process. The Buyer reserves the right to accept or decline such changes.

3.7 Secondary Function

3.7.1 The secondary function of PET is to provide 3rd line support for the Crime IdAM systems live service which operates Monday to Friday 08:00 hours to 18:00 hours ('Support').

3.7.2 The Crime IdAM service is operational 24/7 and core 3rd line support will be provided between 08:00 hours and 18:00 hours. (Monday to Friday).

3.7.3 Additional on-call out of hours 3rd line support is required between 18:00 hours and 20:00 hours. (Monday to Friday).

3.7.4 Saturday on-call out of hours support is required between 08:00 hours and 16:00 hours.

3.7.5 24/7 support would not be expected to be a requirement within the term of the contract.
3.7.6 1st and 2nd line support is being performed by the Buyer's Service Desk and Application Management team, where the majority of support calls by users are handled and resolved.
3.7.7 Communication between the Crime IdAM PET Team, 2nd and 3rd Line Support is through the HMCTS Delivery Manager and via ServiceNow and JIRA.

3.8 Delivery Management & DevOps

3.8.1 To avoid or mitigate the impact of conflict between the functions (as whilst one function strives to maintain a stable system, the other function may upset that stability through the provision of Enhancements) the service must operate to an effective DevOps driven operating model ('Delivery Management'). This outcome will be implicit in the delivery of the Primary and Secondary Functions and the entire requirement delivered as a seamless whole.
3.8.2 The current PET MSP supports the following work within the current backlog and, although the volume of users is expected to increase, it is not anticipated that this will have significant impact during the term of the contract.
3.8.3 Current Backlog

The following information is an example of the work currently on the Crime IdAM backlog:

- Complete ForgeRock upgrades
- Migrate from RHEL to Ubuntu
- CaTH integration (multiple environment integration)
- Assess migration to managed PostgreSQL instance.
- Support release 5.12.0 live environment deployment support and non-live environment deployment.
- Limit Organisation Admin permissions
- Crime IdAM back-ups – 90-day retention
- Remove any old Java 8 images from Jenkins.
- Change password length from 8 to 12 characters.
- Remove password reset requirement.
- Remove user and organisation data from PostgreSQL.
- Update terms and conditions
- Upgrade Java
- ITHC recommendations and preparation for next ITHC.
- Upgrade to IDM 7.3.

4.9 Knowledge Management

4.9.1 Potential Provider shall ensure that knowledge is developed, maintained and retained in order to maintain a good quality service to the Buyer during the term of the contract in order to fulfil and meet the demands of HMCTS with no impact to the Buyer.

Supplier's Tender Response

[REDACTED]

Attachment 2 – Charges and Invoicing

Part A – Milestone Payments and Delay Payments

[REDACTED]

Crown Commercial Service

#	Milestone Description	Activities/Deliverables:	Milestone Payment amount (£GBP)	Target Milestone Date	Delay Payments (where Milestone) (£GBP per day)
M1	October 2024 transition and knowledge transfer activities undertaken by the Supplier in accordance with the Outline Implementation Plan.	• Supplier attendance at knowledge transfer sessions scheduled in October 2024 with the incumbent supplier and the Buyer.	[REDACTED]	31st October 2024	N/A
M2	November 2024 transition and knowledge transfer activities undertaken by the Supplier in accordance with the Outline Implementation Plan.	• Supplier attendance at knowledge transfer sessions scheduled in November 2024 with the incumbent supplier and the Buyer. • Written confirmation from the Supplier that knowledge transfer activities with the incumbent supplier are complete. • Acceptance into Service (AiS) activities completed.	[REDACTED]	30th November 2024	N/A

Part B – Service Charges

Service Charges shall be subject to Indexation using the Consumer Price Index and only applied following the Initial Term, such that the first adjustment will apply from the second anniversary of the Commencement Date and on the anniversary of the Commencement Date in subsequent Contract Years.

[REDACTED]

[REDACTED]

Crown Commercial Service

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

The Rate Card shall be subject to Indexation. using the Consumer Price Index and only applied following the Initial Term, such that the first adjustment will apply from the second anniversary of the Commencement Date and on the anniversary of the Commencement Date in subsequent Contract Years.

Staff Grade	Day Rate (£)
Delivery Manager	[REDACTED]
Solution Architect	[REDACTED]
Technical Lead	[REDACTED]
Full Stack Engineer	[REDACTED]
Web/DevOps	[REDACTED]
Quality Assurance	[REDACTED]
Frontend Developer	[REDACTED]
Dev/Ops	[REDACTED]

Crown Commercial Service

Part D – Risk Register

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)

1. In the event that the Buyer terminates this Call Off Contract, in whole or in part, pursuant to Clause 35.1.9 (Termination without Cause), the Buyer shall pay to the Supplier costs in respect of costs incurred by the Supplier exclusively in respect of Services being provided under this Call Off Contract which cannot be cancelled without Losses being incurred where the following conditions apply:
    1. the Supplier has used all reasonable endeavours to mitigate the Losses;
    2. full disclosure of information to support the Loss is provided; and
    3. No element of overhead recovery or profit is added to the Loss.

[REDACTED]

Crown Commercial Service

2. No other termination or compensation payments shall be payable in relation to the termination or expiry of this Call Off Contract.

Crown Commercial Service

Attachment 3 – Outline Implementation Plan

Dates and timelines are deemed to be targets only.

[REDACTED]

In accordance with the Outline Implementation Plan, transition and knowledge transfer is estimated to be a 7 (seven) week duration. The total Contract Period (if the optional Extension Periods are implemented) will therefore comprise of an estimated 7 (seven) weeks of transition and 251 weeks of “run”.

[REDACTED]

Crown Commercial Service

Attachment 4 – Service Levels and Service Credits

1. DEFINITIONS

1.1 In this attachment, the following words shall have the following meanings and they shall supplement Schedule 1 (Definitions):

[REDACTED]

Crown Commercial Service

2. **SERVICE LEVELS:**

Clock Stop:

[REDACTED]

Amendments to the Call Off Terms:

[REDACTED]

Calculation of Service Credits

[REDACTED]

3. **PERFORMANCE INDICATORS:**

The below are Performance Indicators only and the Supplier shall have no liability for Service Credits for failure to achieve the targets set out below. The KPIs shall be measured and reported quarterly:

	KPI Description	Good Target	Approaching Target Threshold	Requires Improvement Threshold	Inadequate Threshold
1	MAC 2.3 Tackling economic inequality through training (50 hours) – See Supplier Master Social Value KPI Return Template	96% (48 hours)	90% (45 hours)	80% (40 hours)	76% (38 hours)
2	MAC 4.1 Fighting climate change through volunteering (10 hours) – See Supplier Master Social Value KPI Return Template	90% (9 hours)	80% (8 hours)	70% (7 hours)	65% (6.5 hours)

Attachment 5 – Key Supplier Personnel and Key Sub-Contractors

.1.5 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

[REDACTED]

Key Supplier Personnel	Key Role(s)	Duration
	Vice President Consulting Services	Contract Period
	Director Consulting Services	Contract Period

Part B – Key Sub-Contractors

Key Sub-contractor name and address (if not the same as the registered office)	Registered office and company number	Related product/Service description	Key Sub-contract price expressed as a percentage of total projected Charges over the Contract Period	Key role in delivery of the Services
N/A				

Crown Commercial Service

Attachment 6 – Software – NOT APPLICABLE

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

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

Part A – Supplier Software

The Supplier Software includes the following items:

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

Crown Commercial Service

Part B – Third Party Software – 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
N/A							

Attachment 7 – Financial Distress

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

PART A – CREDIT RATING THRESHOLD

[REDACTED]

PART B – LONG FORM GOVERNANCE – NOT USED

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

Not Applicable.

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

[REDACTED]

Attachment 10 – Transparency Reports

Title	Content	Format	Frequency
Sprint Report		Confluence Report	[REDACTED]
Call-Off Contract Charges			[REDACTED]
Performance Report against stated SLA including Service Now Reports			[REDACTED]

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

FRAMEWORK SCHEDULE 4 – ANNEX 2

RM6100 TECHNOLOGY SERVICES 3

LOTS 2, 3 AND 5 CALL OFF TERMS

[REDACTED]