I DISPUTES AND LAW

I1 Governing Law and Jurisdiction

I1.1 Subject to the provisions of clause I2 the Contract, including any matters arising out of or in connection with it, shall be governed by and interpreted in accordance with English Law and shall be subject to the jurisdiction of the Courts of England and Wales. The submission to such jurisdiction shall not limit the right of the Authority to take proceedings against the Contractor in any other court of competent jurisdiction, and the taking of proceedings in any other court of competent jurisdiction shall not preclude the taking of proceedings in any other jurisdiction whether concurrently or not.

I2 Dispute Resolution

I2.1 The Parties shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the Contract within 20 Working Days of either Party notifying the other of the dispute and such efforts shall involve the escalation of the dispute to the finance director of the Contractor and the commercial director of the Authority.

I2.2 Nothing in this dispute resolution procedure shall prevent the Parties from seeking from any court of competent jurisdiction an interim order restraining the other Party from doing any act or compelling the other Party to do any act.

I2.3 If the dispute cannot be resolved by the Parties pursuant to clause I2.1 the Parties shall refer it to mediation pursuant to the procedure set out in clause I2.5 unless: (a) the Authority considers that the dispute is not suitable for resolution by mediation; or (b) the Contractor does not agree to mediation.

I2.4 The obligations of the Parties under the Contract shall not cease, or be suspended or delayed by the reference of a dispute to mediation (or arbitration) and the Contractor and the Staff shall comply fully with the requirements of the Contract at all times.

I2.5 The procedure for mediation and consequential provisions relating to mediation are as follows:

(a) a neutral adviser or mediator (the **"Mediator"**) shall be chosen by agreement between the Parties or, if they are unable to agree upon a Mediator within 10 Working Days after a request by one Party to the other or if the Mediator agreed upon is unable or unwilling to act, either Party shall within 10 Working Days from the date of the proposal to appoint a Mediator or within 10 Working Days of notice to either Party that he is unable or unwilling to act, apply to the Centre for Effective Dispute Resolution to appoint a Mediator;

(b) the Parties shall within 10 Working Days of the appointment of the Mediator meet with him in order to agree a programme for the exchange of all relevant information and the structure to be adopted for negotiations. If appropriate, the Parties may at any stage seek assistance from the Centre for Effective Dispute Resolution to provide guidance on a suitable procedure;

(c) unless otherwise agreed, all negotiations connected with the dispute and any settlement agreement relating to it shall be conducted in confidence and without prejudice to the rights of the Parties in any future proceedings;

(d) if the Parties reach agreement on the resolution of the dispute, the agreement shall be recorded in writing and shall be binding on the Parties once it is signed by their duly authorised representatives;

(e) failing agreement, either of the Parties may invite the Mediator to provide a non-binding but informative written opinion. Such an opinion shall be provided on a without prejudice basis and shall not be used in evidence in any proceedings relating to the Contract without the prior written consent of both Parties; and

(f) if the Parties fail to reach agreement in the structured negotiations within 60 Working Days of the Mediator being appointed, or such longer period as may be agreed by the Parties, then any dispute or difference between them may be referred to the Courts unless the dispute is referred to arbitration pursuant to the procedures set out in clause I2.6.

I2.6 Subject to clause I2.2, the Parties shall not institute court proceedings until the procedures set out in clauses I2.1 and I2.3 have been completed save that:

(a) The Authority may at any time before court proceedings are commenced, serve a notice on the Contractor requiring the dispute to be referred to and resolved by arbitration in accordance with clause I2.7;

(b) if the Contractor intends to commence court proceedings, it shall serve notice on the Authority of its intentions and the Authority shall have 21 days following receipt of such notice to serve a reply on the Contractor requiring the dispute to be referred to and resolved by arbitration in accordance with clause I2.7; and

(c) the Contractor may request by notice to the Authority that any dispute be referred and resolved by arbitration in accordance with clause I2.7, to which the Authority may consent as it sees fit.

I2.7 If any arbitration proceedings are commenced pursuant to clause I2.6,

(a) the arbitration shall be governed by the provisions of the Arbitration Act 1996 and the Authority shall give a notice of arbitration to the Contractor (the "**Arbitration Notice**") stating:

(i) that the dispute is referred to arbitration; and

(ii) providing details of the issues to be resolved;

(b) the London Court of International Arbitration (**"LCIA"**) procedural rules in force at the date that the dispute was referred to arbitration in accordance with I2.7(b) shall be applied and are deemed to be incorporated by reference to the Contract and the decision of the arbitrator shall be binding on the Parties in the absence of any material failure to comply with such rules;

(c) the tribunal shall consist of a sole arbitrator to be agreed by the Parties;

(d) if the Parties fail to agree the appointment of the arbitrator within 10 days of the Arbitration Notice being issued by the Authority under clause I2.7(a) or if the person appointed is unable or unwilling to act, the arbitrator shall be appointed by the LCIA;

(e) the arbitration proceedings shall take place in London and in the English language; and

(f) the arbitration proceedings shall be governed by, and interpreted in accordance with, English Law.

IN WITNESS of which this Contract has been duly executed by the parties.

SIGNED for and on behalf of **CARE QUALITY COMMISSION**

Signature [redacted] .....

Name ..[redacted] .....

Position . .....

Date ..2[redacted] .....

SIGNED for and on behalf of **[CONTRACTOR]**

Signature [redacted] .....

Name ....

Position . .....

Date 16[redacted] .....

SCHEDULE 1 - SPECIFICATION

Statement of Requirements

1. THE REQUIREMENT

CQC is seeking a contract to provide them with the full administration of on-line applications for disclosure and barring service checks as well as the essential requirement of a national ID checking service specifically designed for CQC staff (such as the Post Office ID checking service).

This needs to include specific information relevant to the applicants role, in a drop down format within the online application and should include CQC specific information such as Job Role, Location, and Directorate, In addition, CQC are also seeking access to the provision of advice on DBS policies and procedures, as laid down by the Disclosure and Barring Service.

As part of the service provision, CQC will require both the user DBS applicant and Human Resources to have full access to a CQC branded site to enable us to send and monitor applications, as well as access to a full management information reporting function to enable us to manage ongoing applications, verify and track all applications within the checking process including initial confirmation confirming if a check is clear or contains information. CQC must therefore be able to access this information in-house and online.

The contractor shall be registered with the Disclosure and Barring Service (DBS) to administer disclosure applications on behalf of non-registered organisations using the DBS e-bulk service interface. The contractor shall deliver the contract requirements securely and in compliance with Disclosure and Barring Service procedures. They shall have fully developed and tested business continuity and disaster recovery plans for the system and premises.

Existing Process for DBS Checks

Below is a high-level outline of the existing process which CQC follows for initiating, progressing and completing its DBS checks:

Step 1 - Applicant is sent an invite to complete a DBS:
Step 2 - Applicant completes the online form
Step 3 - Applicant prints off letter and takes it to the post office to verify ID
Step 4 - Post office confirms ID to contractor
Step 5 - Contractor submits application to DBS
Step 6 - DBS carries out checks
Step 7 - Applicant and CQC receive confirmation of checks
Step 8 - CQC access progress of applications and results via the online management reporting system.

National ID Checking Service

As part of the service provision, CQC also require a national ID checking service specifically designed for its staff. CQC's existing service provision utilises the Post Office Identity Checking Service for applicants applying online. The applicant is asked to specify which forms of ID (from the approved DBS list) they will use. The applicant prints off a barcoded letter and takes this to a participating Post Office (usually Crown) where Post Office staff scan and follow the instructions on screen to check the original documents presented to them. The ID is returned to the applicant and the results of the checks are sent back to the contractor electronically.

Indicative Forecast Volumes

Indicative forecast volumes for fully processed disclosure applications are described below:

CQC Workforce Group	Indicative Volume for 2017/18	Indicative Volume for 2018/19	Indicative Volume for 2019/20
Flexible Workforce	3043	1223	800
Permanent Workforce	531	1117	1054
Combined anticipated minimum applications	>500	>500	>500

PLEASE NOTE: Tenderers should be aware that the volumes outlined above are indicative forecasts, and may be subject to fluctuation (for example, if there are changes in staff headcount numbers). **Please therefore note that CQC cannot guarantee this level of business.**

Availability of Service

Tenderers are required to provide details of any regular downtime they will require to maintain the system during which periods applicants' and CQC's access to the system may be nil or constrained. CQC's preference is that this should occur outside of working hours (e.g. between midnight – 6am) but this is negotiable.

The Contractor must provide a minimum of two working days' notice of any other downtime outside this schedule.

CQC accepts that there may be occasions where the work may exceed the allotted time. In these cases the Contractor is required to minimise any overrun. CQC also accepts that there may still be occasions where more extensive scheduled work or unplanned emergency outages occur. The Contractor is required to minimise the occurrence and impact of these occasions, which should not exceed 24 hours per rolling three month period.

CQC also expect that the contractor will provide access to a helpline which is contactable between 0900 hours and 1700 hours, Monday to Friday excepting public holidays.

Data Security & Management

The contractor must evidence their e-bulk registration with DBS and that they meet all technical requirements set by DBS. The contractor will be responsible for the secure receipt, storage, dissemination and destruction of disclosure application forms, supporting documentation and disclosures, in line with CQC's requirements incorporating the DBS Code of Practice.

The contractor must comply with the following requirements:

a. Compliance with the Data Protection Act 1998 (DPA)

b. Explain their approach to protecting personal information and whether they hold any relevant certifications (e.g. Cyber Essentials, Cyber Essentials Plus, ISO27001)

c. Provide the nominated Contract Manager (or equivalent) within CQC with lifecycle maps of processes, which may be subject to annual review by CQC (with any identified changes to be agreed between the Contractor and CQC as part of the variation process)

d Comply with a documented route for reporting incidents which affect, or may affect, the confidentiality, integrity or availability of CQC data.

e. Undertake all necessary action to address and resolve any issues identified through any of the above processes. Outputs and timescales to be agreed with the nominated CQC Contract Manager (or equivalent)

Any staff employed on the work of this contract must ensure that agreed procedures are fully adhered to and such activity is auditable by CQC as part of the contract.

If subcontractors will be used on the work of this contract, tenderers must provide full details and explain how they will ensure that the subcontractors will consistently meet the appropriate security requirements. This information should be provided as part of the tender. Any new subcontractors must be agreed by the CQC Contract Manager (or equivalent).

Tenderers should provide details of the processes they will employ to ensure these requirements are met and any actions they will take if any breaches of security are identified. Details must also be provided of any known breaches which tenderers have incurred on this nature of work, and any resulting action taken.

The Contractor will be required formally to notify CQC immediately of any breach of security being identified. Such notification must be provided to CQC's nominated Contract Manager and any other relevant function/team within CQC, to be advised after contract award.

Contingency Planning (Business Continuity and Disaster Recovery)

The contractor must provide fully developed and tested plans separately for business continuity and disaster recovery for their operation. They must also provide details of a review schedule for these plans. This should cover specific details of the procedures to be invoked to facilitate the full restoration of their operation including how long it would take to resume a full service. The Contractor shall comply at all times with the relevant provisions of the Business Continuity and Disaster Recovery Plan, and this will be incorporated into the final contract.

The Business Continuity and Disaster Recovery Plan shall be compliant with current International Standards ISO 22301 and ISO 22313 (or equivalent). In particular the Business Continuity and Disaster Recovery Plan must show that the Contractor is able to maintain the Services throughout the terms of the contract as far as practicable in the event of a Disaster, unforeseen business disruption or emergency event.

Duration of Contract

The contract that CQC intends to award will cover a period of 3 years, with the opportunity for this to be extended by up to a further 1 year (subject to agreement by both parties).

3. AUTHORITY RESPONSIBILITIES

As part of the overall contract, CQC shall:

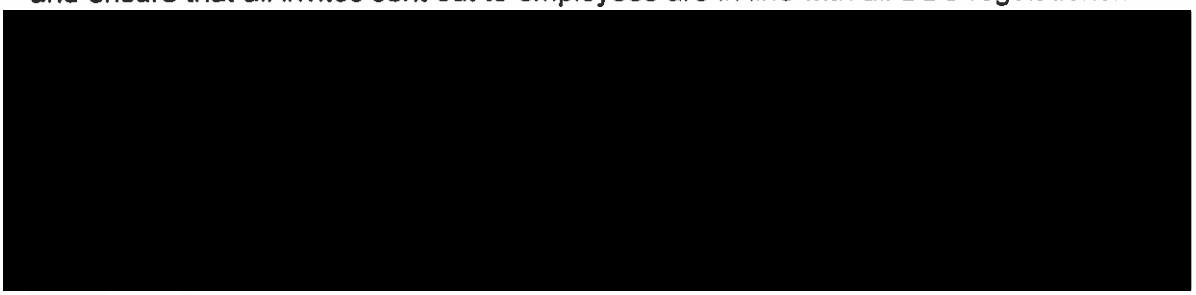
• Nominate a lead within the organisation to oversee the delivery of the service from an internal perspective and to report ad hoc issues, requests and amendments, as required Attend meetings

with the supplier, e.g. on an annual, biannual, or quarterly basis (to be determined with the supplier) to formally review the service and ensure that it remains compliant with CQC's requirements (in line with the specification) Any expenses incurred through travel and subsistence will be met by the contractor

• Where relevant, provide opportunities for internal users of the service to share feedback about it via the nominated lead to ensure it remains fit for purpose

With specific regard to the E-Service, CQC's HR Team will be responsible for sending all invites to staff that are required to complete a DBS check, and will continually monitor the E service through the contractor's portal to ensure staff compliance. CQC will also run monthly reports to verify applications that haves been processed through the portal and to check on average time frames from invitation to result received.

The following individuals will be responsible for the daily management of the E-service with CQC and ensure that all invites sent out to employees are in line with all DBS regulations:.



The CQC is an Agency for the Department for Health and is therefore a public body. As such, CQC must respond to any request for information under the Freedom of Information Act (2000). Any information held by or on behalf of CQC may be requested and disclosed to members of the public, but only in a manner compatible with the legislation. Should any information be requested that refers to the contractor or any tender application, CQC will inform the specific organisation as appropriate.

4. CONTRACTOR RESPONSIBILITIES

The contractor must be an approved registered provider with the Disclosure and Barring Service, who can administer disclosure applications. Evidence should include listing on https://www.gov.uk/find-dbs-umbrella-body and evidence of registration with DBS as an e-bulk provider.

The contractor and is required to have in place an electronic interface for submitting applications to DBS (commonly known as e-Bulk). The system should fully meet DBS's criteria and allow applicants to log into the system remotely to complete their application online before submitting it to the contractor electronically.

The system must be remotely accessible to nominated individuals within CQC and be able to show the results of the DBS check in a clear and easy to understand format. The minimum data fields required by CQC are:

• Title;
• Forename;
• Surname
• Address
• Job title
• Directorate, in line with CQCs structure.
• Date of birth
• Disclosure reference number

• Disclosure issue date
• Confirmation if an application holds information regarding a criminal conviction. Such data should be available to CQC to export into an approved format e.g. Microsoft Excel

The contractor must also:

• have a full and demonstrable understanding of the DBS disclosure and barring service processes and procedures;
• provide ongoing support on a daily basis to the CQC HR services, Flexible workforce team to assist and answer any issues arising on a daily basis, between the hours of 9:00am (09:00) to 5:00pm (17:00);
• provide CQC HR with a bespoke interface to enable access to an online CQC branded site, so staff have confidence that personal information is being provided and managed securely and to enable them to access information such as job title from a list specific to the relevant roles in CQC (CQC to provide supplier with a list of relevant roles/job titles);
• have direct links to the DBS policy team to assist in higher level queries relating to the DBS checking requirements of CQC;
• Act as a countersignature to CQC in progressing applications; and
• Provide monthly Management meeting to ensure any changes to the system
or DBS rules are provided to enable CQC to respond and act within the rules and regulations of the Disclosure and Barring Service.

CONTRACT MANAGEMENT AND MONITORING

CQC will appoint a nominated Contract Manager (or equivalent) who will oversee key performance indicators on a monthly basis with the contractor.
The contractor will be required to provide a meeting and activity reports to enable CQC to monitor:
• Number of applications in progress at each stage of the DBS check
• Report on costs
• Progress in delivering the requirement:

Key performance indicators will include

Key Performance Indicator (KPI)	Frequency	Threshold
Completed applications passed to DBS	As and When	3 days
Query response time frame (HR team)	As and when	2 days
Chase up outstanding DBS applications within their agreed SLAs	when identified	As defined by the Disclosure and Barring service time frames (after 60 days)
Update system in line with DBS information, in line with contract SLAs	as and when	Within 2 working days (or as jointly determined between CQC and the Supplier)
Add and remove new user accounts	As and When	2 working days
Respond to applicant queries	As and When	*2 working Days*

To monitor progress against the KPIs, the contractor must provide and agree the following with CQC:

- Performing quality assurance on all aspects of the requirement;
- Provide CQC with timely and ongoing evaluation and quality assurance information relating to the service;
- Monitor the quality of the service provision to ensure customer satisfaction in accordance with the KPIs outlined in the Contract, unless otherwise approved by the Contract Manager;
- Attend a post contract review with CQC to review whether the objectives of the contract were met, to review the service and to identify any lessons learnt for future projects.

TIMETABLE

It is envisaged that the service will commence from April 2017 (subject to agreement of the final contract between CQC and the incoming service provider); following this support will be required on an ongoing basis throughout the length of the contract.

SKILLS AND KNOWLEDGE TRANSFER

There are clear benefits for a DBS E Service to be provided by an external provider, the resource required to dedicate timely advice and support, but also taking into account the sensitivities around why we are providing this support. However, we will work closely with the provider throughout the working relationship and monitor and propose ways of upskilling the team wherever possible when exiting the contract.

Following completion of the contract and any post-contract review meeting with the supplier (assuming one is held), a summary will be produced by CQC of its delivery, including against the key performance indicators and whether lessons could be learnt, for internal reference. This is to

ensure that future contracts of this nature can achieve maximum customer satisfaction and value for money. This summary will be shared with the supplier, upon request.

8. Further Information

Acceptance of Tender

CQC does not bind itself to accept any tender, and CQC reserves the right at any time:

(a) To issue amendments or modifications to the ITT during the tender period;
(b) To clarify tenders once these have been submitted;
(c) To alter the timetable to contract award;
(d) Not to award a contract; and/or
(e) To withdraw from this procurement process

Please note that any costs or expenses incurred in the preparation of a tender response by any bidder or other person will not be reimbursed by CQC and CQC will in no way be liable to any bidder or other person for any costs, expenses or losses incurred by any bidder or other person in connection with this tender process or at all.

Training & Support

The successful contractor will be required to provide relevant training to CQC staff listed in to enable them to use the system but information to confidently offer advice to CQC staff using the system to apply for a DBS.

Point of Contact for Contractual Matters

For matters relating to the contract, the Point of Contact authorised to act as CQC's representative is:

Commercial & Contracts Team
Care Quality Commission
Citygate
Gallowgate
Newcastle upon Tyne NE1 4PA

Payment

The contractor will be expected to handle all payments to DBS for the cost of an enhanced disclosure, for subsequent reimbursement by CQC, and tenderers should outline the process by which these payments will be made. The contractor shall invoice CQC monthly in arrears. CQC operates a Purchase Order scheme for payment of invoices. Full instructions will be issued to the successful contractor. In essence, the contractor will be supplied with a Purchase Order number which must be quoted on each invoice submitted to CQC's Shared Service Centre. All invoices must quote a purchase order number, in order to effect payment of all correct invoices within 30 working days.

All invoices must be posted to the address below:

Care Quality Commission
T70 Payables F175
Phoenix House, Topcliffe Lane
Wakefield, West Yorkshire
WF3 1WE

SCHEDULE 2 – TENDER RESPONSE

RESPONSE TO TECHNICAL EVALUATION REQUIREMENT STATEMENTS

Tenderers must provide responses to the Technical Evaluation Requirement Statements below, to describe how they will meet the requirements of the contract. Questions should be answered in full and should not refer to other documents or appendices (unless otherwise instructed).
Tenderers are referred to the Statement of Requirements when forming responses, and reminded that the Technical Evaluation will account for 60% of their total tender score.

	Requirement Statements	Question Weighting
	Overview Tenderers must provide a concise summary highlighting the key aspects of the proposal. **Please note:** Tenderers must not submit marketing material or any other documents (other than any supporting documents requested by CQC as part of their tender submission)	This response is not evaluated and should be used to contextualise the Tenderer' s response.
	Response: Atlantic Data Ltd (ADL) is proposing to continue to provide a smooth process and comprehensive solution for the Care Quality Commission (CQC) to process and manage its criminal records checking requirements, throughout the organisation. ADL has been working with CQC for several years and would welcome the opportunity to continue to provide its ***Disclosures Manager*** system and associated services as a result of this invitation to tender. This proposal sets out a streamlined process whereby users can sign into the Disclosures Manager by visiting an internet-based system to log-in using their given credentials. The Disclosure Manager system has several in-built features such as reporting suites, Post Office ID checking, instant Route 2 ID checking, in-line help and system guidance notes. Internal CQC users are instantly informed once the result is issued by the DBS. ADL would be happy to consider, assess and develop any additional features to the	

Requirement Statements		Question Weighting
	existing system based on CQC's request.	

	METHOD STATEMENT - PROVISION OF SERVICE REQUIREMENTS **Please describe (with specific reference to the key elements within the specification) how it is intended to deliver the service requirements of CQC as outlined within the Invitation to Tender** Evaluation Intention: This criterion seeks to establish that the Tenderer has demonstrated that it has: (a) a credible DBS E-Service solution (which includes the provision of a bespoke portal to CQC and its staff, a national ID checking service, provision for initial telephone diagnostic discussions and the provision of a telephone helpline to assist applicants and CQC's HR Services to resolve issues arising with DBS applications) (b) a full understanding of the Disclosure and Barring Service rules and (c) a demonstrable understanding and appreciation of the role of CQC as a regulatory body, and the importance of DBS criminal record checks & barring lists to the work CQC carries out (d) defined and achievable timescales for delivery of work (e) a comprehensive and feasible approach to service implementation **Please note:** Tenderers must provide evidence of their E-Bulk registration with DBS and that all technical requirements set by DBS have been met. The response may also be supported by providing examples/evidence of similar services previously delivered on behalf of organisations of a similar standing to CQC (in size/profile) and with similar volumes of DBS checks to those indicated within the Invitation to Tender	25%
	Response: ADL is proposing to continue to provide its 'umbrella body' service, known as Disclosures Manager. This is an outsourced service where the applications are processed electronically and the final countersigning is done by ADL. ADL would	

retain the direct contact with the DBS in respect of these CQC's applications.

[redacted] costs for the CQC. ADL charge an annual maintenance of [redacted] There is also an administration fee per application of [redacted] inc. VAT). The admin fee includes a disbursement to the Post Office for their ID checking service. The system would be branded with the CQCs logo, and would include management information and reporting functions to assist with tracking and administering applications.

The Disclosures Manager system is user friendly and very easy to navigate. CQC staff, Human Resources and other system users can visit an assigned URL and log in to the Disclosures Manager portal with their given usernames and passwords. This will give them access to the portal and the ability to carry out functions appropriate to their role.

Job roles relevant to CQC will be stored within the database. The appropriate attributes required by the DBS are assigned to each role. For example, the correct level of DBS check, the correct 'workforce', whether the role is (or could be) a volunteer position for DBS purposes, and whether the role could be a home-based one.

Disclosures Manager is built with a full suite of management reports. There are 10 or more standard reports to help with tracking applications from start to finish, giving timely updates and accessing historical management information. HR or administrative officers of CQC can check the status of all applications along with verifying and tracking the information.

The Post Office ID checking facility within the system will enable CQC staff to complete ID checks nationally without any constraints. The fully submitted applications are usually countersigned on the same day and submitted to the DBS overnight.

The ADL system informs users instantly when an applicant's result is issued by the DBS. Upon receiving the result, Disclosures Manager states whether a certificate is clear or contains information.

ADL has a well-tested and proven disaster recovery and business continuity plan.

In compliance with DBS ID checking requirements, Disclosures Manager also includes an integrated Route 2 ID checking service provided by Experian. Each such application would be charged at [redacted]

To summarise, Disclosures Manager includes:

- Full administration of an on-line process for DBS applications
- CQC-specific applicant roles configured in the system with the appropriate level of DBS check predetermined
- corporate branding
- validation of the data to ensure accuracy and completeness
- the option to integrate with other CQC systems, such as HR or finance to reduce data entry
- save on set-up cost and time involved as system is already in use
- national ID checking via Post Office branches

Compliance

ADL is one of the DBS test partners. As such, ADL works with the DBS to test, perfect and apply legislation changes and technology updates before they are implemented nationally.

ADL complies with all relevant data protection legislation, guidance and best practice to manage, store and share data. ADL is fastidious in its approach to compliance with the DBS Code of Practice and its responsibilities as DBS-approved umbrella body and e-Broker.

ADL is ISO 27001 certified for information and data security.

PO ID checking

ADL understands that as the independent regulator of all health and adult social care services in England, CQC applicants can be dispersed across the country. For CQC's convenience, ADL offers a facility for applicants to complete their applications remotely (e.g. at home) and have their ID checks completed by the Post Office.

To complete a check with the Post Office, applicants log into Disclosures Manager remotely, select the ID documents they'll provide and complete the Applicant's Section of the form. Upon completion, the applicant prints out a system-generated letter. The applicant takes this letter to their local Post Office branch. There, the Post Office scans a barcode on the letter which requests the relevant ID documents from the applicant. The Post Office conducts the ID check, and the applicant's information is transmitted to ADL.

Applicants are required to pa[redacted]t the Post Office.

Account Management

ADL would assign to the CQC a dedicated account manager and access to technical support. The account manager is supported by a client services team. These resources are available for day-to-day operational issues from 9am to 5pm Monday to Friday by telephone or e-mail.

The account manager would handle more significant client issues in a regular review meeting. This account management meeting would have a set agenda, which would include updates on DBS-related news, issues and contract performance. Time would always be devoted to any issues the client may have.

Not only is the account manager supported by a team of experienced account managers and relationship managers with a combined 23 years of DBS experience, they can draw on other expertise from within ADL, such as a compliance team, L&D and technical support.

Evidence of e-broker registration and technical requirements

Please click on the below link to confirm ADL's status as a DBS-approved e-Broker:

https://www.gov.uk/guidance/e-bulk-submitting-multiple-applications-for-dbs-checking-formerly-crb

This registration is clear evidence of ADL's compliance with DBS technical requirements.

Service implementation

As CQC is ADL's existing client, the planning and implementation of Disclosures Manager will not be necessary. This will save incalculable amounts of time, money and resource for the CQC. However, as requested the below provides some details of ADL's approach to service implementation.

Planning

Whenever ADL is fortunate enough to be selected as the supplier for an organisation's DBS checks, it works with a project team from the organisation. ADL closely project manage the planning and service implementation, setting actions and deadlines to ensure that all milestones are achieved and the system is delivered in a timely and controlled manner. ADL initiate a series of weekly project management calls for the duration of the implementation phase.

ADL's project planning and management strategies are based on the waterfall methodology. This is a sequential design process that moves logically through the

following stages: requirements, design, integration, testing and maintenance.

Service Implementation

Based on this methodology, ADL has developed a simple and effective implementation plan. An example of the key stages of a typical implementation are as follows:

• ADL provide a template so that the organisation can provide required information about its locations, applicant's roles and other salient information about the organisation.

• ADL then build, test and demo the Discloses Manager system.

• ADL then pilot the system with a select group of central users.

• Finally, ADL roll-out the system in accordance with an agreed plan to the organisation's wider stakeholders.

This method mitigates project risks because ADL's implementation team guides projects through predetermined phases (with benchmarks) that keep them on track.

Evidence of work for similar organisations

Umbrella Body Clients:

Sl. No.	Client name	Number of applications per year
1	[redacted]	[redacted]
1		
2		
3		
4		
5		

ADL has in excess [redacted] clients ranging from N[redacted]
Councils, national regulatory bodies to SMEs.

CONTRACT MANAGEMENT

Please describe (with specific reference to the key elements within the specification) how it is intended to deliver effectively against the contract management requirements outlined within the Invitation to Tender

Evaluation Intention:

This criterion seeks to establish that the Tenderer has demonstrated that it has:

(a) appropriately qualified and experienced resource to meet the contract management requirements
(b) suitable arrangements for internal monitoring of adherence to defined Key Performance Indicators
(c) identified and proposed suitable management arrangements for any/all delivery risks
(d) a quality assurance regime that monitors, measures and assures quality outcomes.

15%

Response:

As pioneers in the provision of electronic criminal record checks in the UK, ADL has teams of experts in the realms of software development, account management, technical support, legal and compliance to meet the contract management and KPI's indicated in the requirements.

Account Management

ADL would assign to the CQC a dedicated account manager, who is supported by a client services team. These resources are available for day-to-day operational issues from 9am to 5pm Monday to Friday by telephone or email.

The Disclosures Manager system contains comprehensive information to allow the CQC to measure its KPIs. In addition to this, the account manager would schedule regular account management meetings to help CQC to oversee management of the service. This includes providing management information and activity reports to measure key performance indicators, including, but not limited to:-

a. Number of applications in progress at each stage of the DBS check

b. Report on costs

c. Progress in delivering the service

To further monitor progress against the KPIs, ADL would be delighted work with the

	CQC to devise the following: a. Perform quality assurance on all aspects of the requirement b. Provide CQC with timely and ongoing evaluation and quality assurance information relating to the service c. Monitor the quality of the service provision to ensure customer satisfaction in accordance with the KPIs outlined in the Contract d. Attend a post contract review with CQC to review whether the objectives of the contract were met	

SERVICE RESILIENCE/BUSINESS CONTINUITY & DISASTER RECOVERY

Please describe your organisation's approach to disaster recovery and business continuity as a provider of a full e-service for DBS checks.

Evaluation Intention:

This criterion seeks to establish that the Tenderer has described and evidenced:

(a) robust plans for disaster recovery and business continuity;
(b) the resilience of their service provision.
(c) Suitable arrangements for information being transferred between CQC and the contractor

The response may be supported by providing evidence of business continuity plans, which cover aspects such as (but not limited to) power/system failure, major security incidents, peaks in service demand, and contingency arrangements

Response:

15%

ADLs Disaster Recovery Plan (DRP) and Business Continuity Plans (BCP) define the processes and procedures necessary to support the effective and efficient restoration and recovery of critical functions in the event of a disaster, including (but not limited to) power/system failure, major security incidents, peaks in service demand, and contingency arrangements [redacted]

[redacted]

SCHEDULE 3 – PRICING

Pricing Schedule for Provision of e-services for Disclosure and Barring Services CQC PER 018

Table A	
Volume of DBS Checks per Financial Year	Cost per check (including VAT)
0-500	[redacted]
501-1000	
1001-1500	
1501-2000	
2001-2500	
2501-3000	
3001-3500	
3501-4000	
4001+	

Table B	
Any other costs	Cost (including VAT
Route 2 ID Check	[redacted]
Annual Maintenance	

SCHEDULE 4 - CHANGE CONTROL

Contract Change Note

Contract Change Note Number	
Contract Reference Number & Title	
Variation Title	
Number of Pages	

WHEREAS the Contractor and the Authority entered into a Contract for the supply of [project name] dated [dd/mm/yyyy] (the "Original Contract") and now wish to amend the Original Contract

IT IS AGREED as follows

1. The Original Contract shall be amended as set out in this Change Control Notice:

Change Requestor / Originator		
Summary of Change		
Reason for Change		
Revised Contract Price	Original Contract Value	£
	Previous Contract Changes	£
	Contract Change Note [x]	£
	New Contract Value	£
Revised Payment Schedule		
Revised Specification (See Annex [x] for Details)		
Revised Contract Period		
Change in Contract Manager(s)		
Other Changes		

2. Save as herein amended all other terms of the Original Contract shall remain effective.

3. This Change Control Notice shall take effect from the date on which both the Authority and the Contractor have communicated acceptance of its terms.

SCHEDULE 5 - COMMERCIALLY SENSITIVE INFORMATION

1.1 Without prejudice to the Authority's general obligation of confidentiality, the Parties acknowledge that the Authority may have to disclose Information in or relating to the Contract following a Request for Information pursuant to clause E5 (Freedom of Information).

1.2 In this Schedule the Parties have sought to identify the Contractor's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be contrary to the public interest.

1.3 Where possible the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies.

1.4 Without prejudice to the Authority's obligation to disclose Information in accordance with the FOIA and the EIR, the Authority will, acting reasonably but in its sole discretion, seek to apply the commercial interests exemption set out in s.43 of the FOIA to the Information listed below.

CONTRACTOR'S COMMERCIALLY SENSITIVE INFORMATION	DATE	DURATION OF CONFIDENTIALITY
Details of existing clients		Indefinite
Pricing		Indefinite
Business Continuity and Disaster Recovery plans		Indefinite

SCHEDULE 6 - NON DISCLOSURE AGREEMENT

THIS NON DISCLOSURE AGREEMENT is made the [insert day] day of [insert date] (the "Commencement Date"

BETWEEN:

[Insert full name of contractor] of [insert full address but if registered company please insert the following - (registered in England and Wales under number [insert company number]) whose registered office is situated at [ ] (the "Contractor");

and

[Insert name and address of the Staff member, professional advisor or consultant of the Contractor] (the "Disclosee").

(each a "Party" and together the "Parties").

WHEREAS:

(a) The Contractor has contracted with the Care Quality Commission (the "Authority") to provide services to the Authority in an agreement dated [insert date] (the "Contract").

(b) The Contract places an obligation of confidentiality on the Contractor. The Disclosee is an [insert employee, professional advisor or consultant] of the Contractor engaged in the provision of services to the Authority in support of or in connection with the services to be provided by the Contractor under the Contract.

(c) The Disclosee may therefore, have communicated to it, certain Confidential Information belonging to the Authority which is proprietary and must be held in confidence. Accordingly, the Contract requires the Contractor to ensure that the Disclosee enters into a non-disclosure agreement with the Contractor on the terms set out herein.

(d) Any Confidential Information disclosed by the Authority or the Contractor to the Disclosee, whether contained in original or copy documents, will at all times remain the property of the Authority together with all notes, memoranda and drawings that have been made as a result of access to such Confidential Information.

NOW IT IS AGREED as follows:

Definition and Interpretation

1. In this Agreement:

a) "Confidential Information" means: any information which has been designated as confidential by the Authority in writing or that ought to be considered as confidential (however it is conveyed or on whatever media it is stored) whether commercial, financial, technical or otherwise including (without limitation) information belonging to or in respect of the Authority which relates to research, development, trade secrets, formulae, processes, designs, specifications, the Authority data, internal management, information technology and infrastructure and requirements, price lists and lists of, and information about, customers and employees, all materials and information belonging to third parties in respect of which the Disclosee owes obligations of confidence; information the disclosure of which would, or would be likely to, prejudice the commercial interests of any person, intellectual property rights or know-how of the Authority and all personal data and sensitive personal data within the meaning of the Data Protection Act

1998; whether or not that information is marked or designated as confidential or proprietary; whether arising prior to, on or after the Commencement Date;

b) "Law" means 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 of which the Contractor is bound to comply.

2. In construing this Agreement the general words introduced or followed by the word include(s) or including or in particular shall not be given a restrictive meaning because they are followed or preceded (as the case may be) by particular examples intended to fall within the meaning of the general words.

3. Unless the context requires otherwise, the singular shall include the plural and vice versa, and the masculine shall include the feminine and vice versa.

4. Reference to any legislative and statutory requirement or similar instrument shall be deemed to include reference to any subsequent amendment to them.

5. References to any person shall, as the context may require, be construed as a reference to any individual, firm, company, corporation, government department, agency, or any association or partnership (whether or not having a separate legal personality).

CONFIDENTIALITY

6. The Disclosee undertakes to: keep confidential all Confidential Information and safeguard it accordingly; and that any Confidential Information supplied will not be used by it for any purpose other than in connection with the Contractor's delivery of the services under the Contract without the prior written permission of the Authority.

7. The Disclosee will take all necessary precautions to ensure that the Confidential Information is held in confidence and will provide proper and secure storage for all information and any papers, drawings or other materials which relate to or are compiled from such information.

8. The Disclosee shall, with respect to any Confidential Information it receives directly from or on behalf of the Authority or from the Contractor, comply, with all instructions and/or guidelines produced and supplied by or on behalf of the Authority from time to time for the handling and storage of Confidential Information, generally or for specific items.

9. The Disclosee will not disclose any Confidential Information or any part thereof to any third party.

10. Where the Disclosee is an employee, breach of the obligations set out herein in this Agreement shall be a cause of disciplinary proceedings, and the Contractor shall institute and enforce such disciplinary proceedings as against the Disclosee in relation to such breach.

11. Where the disclose is a professional advisor or consultant, breach of the obligation set out herein shall entitle the Contractor to terminate the contract of engagement with the Disclosee immediately, and the Contractor shall enforce such right of termination as against the Disclosee in relation to such breach.

12. All Confidential Information in tangible form received hereunder together with all copies thereof shall be destroyed or returned immediately to the Contractor or where so required

by the Authority and notified to the Disclosee, to the Authority, upon request or upon completion of the task for the purposes of which such Confidential Information was released.

13. The Confidential Information will not be used by the Disclosee for any purpose or in any way other than under this Agreement.

14. The following circumstances shall not constitute a breach of the obligations of confidentiality contained in this Agreement:

14.1 Disclosure of Confidential Information by the Disclosee when required to do so by Law or pursuant to the rules or any order having the force of Law of any court, of competent jurisdiction;

14.2 Disclosure of Confidential Information by the Disclosee where and to the extent that the Confidential Information has, except as a result of breach of confidentiality, become publicly available or generally known to the public at the time of such disclosure;

14.3 Disclosure of Confidential Information by the Disclosee where and to the extent that the Confidential Information is already lawfully in the possession of a recipient or lawfully known to it prior to such disclosure;

14.4 Possession of Confidential Information by the Disclosee where it has been acquired from a third party who is not in breach of any obligation of confidence in providing that Confidential Information;

provided that, in no event shall information relating to the affairs of any identifiable person be disclosed or released from the obligations herein without the prior written consent of the Authority.

15. The Disclosee shall: notify the Contractor and the Authority promptly of the date and circumstances of the loss or unauthorised disclosure, if any, of the Confidential Information or any part of the Confidential Information and in addition, the action being taken to rectify that loss or unauthorised disclosure.

16. The obligations contained in this Agreement shall continue until notified in writing by the Authority or the Confidential Information becomes public knowledge (other than by breach of the terms of this Agreement).

17. No licence of any intellectual property rights (including but not limited to patent rights, copyrights, trademarks and rights in proprietary information and/or know-how and whether registrable or unregistrable) is granted hereby, beyond that necessary to enable use of the Confidential Information for the purpose for which the Confidential Information was released.

18. Nothing in this Agreement shall be construed as compelling any of the Parties to disclose any Confidential Information or to enter into any further contractual relationship with any other party.

19. No representation or warranties are given regarding the accuracy, completeness or freedom from defects of the Confidential Information or with respect to infringement of any rights including intellectual property rights of others.

20. Without affecting any other rights or remedies that the other Parties may have, the Disclosee acknowledges and agrees that damages alone would not be an adequate remedy for any breach of any of the provisions of this Agreement.

GENERAL

21. No failure or delay by any Party to this Agreement in exercising any of its rights hereunder shall operate as a waiver of such rights, nor shall any single or partial exercise preclude any further exercise of such rights. Any waiver by a Party of any breach or non-compliance with any term of this Agreement shall not constitute a waiver of any subsequent breach of non-compliance with the same or any other term of this Agreement.

22. No Party may assign this Agreement or any of its rights and obligations hereunder without the prior written consent of the Authority.

23. Any notice under this Agreement shall be in writing and shall be delivered by post, fax or e-mail to the address of the Party in question set out at the beginning of this Agreement or such other address (or e-mail address or fax number) as the Parties may notify one another from time to time.

24. No term of this Agreement shall be enforceable, by virtue of the Contracts (Rights of Third Parties) Act 1999, by any person who is not a party to this Agreement other than the Authority. The Parties shall only with the prior written consent of the Authority be entitled to vary any of the provisions of this Agreement without notifying or seeking the consent of any third party and the rights conferred by section 2 of the Contracts (Rights of Third Parties) Act 1999 are excluded.

25. This Agreement shall be governed by and shall be interpreted in accordance with the laws of England.

26. The courts of England have exclusive jurisdiction to settle any disputes which may arise out of or in connection with this Agreement and accordingly that any proceedings, suit or action arising out of or in connection therewith shall be brought in such courts.

This Agreement has been entered into on the date first written above.

SIGNED by the authorised signatory for and on behalf of the Contractor:

_____

SIGNED by the Disclosee:

_____

SCHEDULE 7 - CONTRACTOR AND THIRD PARTY SOFTWARE

CONTRACTOR SOFTWARE

For the purposes of this Schedule 7, "**Contractor Software**" means software which is proprietary to the Contractor, including software which is or will be used by the Contractor for the purposes of providing the Services. The Contractor Software comprises the following items:

Software	Supplier (if Affiliate of the Contractor)	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?
Disclosures Manager							

THIRD PARTY SOFTWARE

For the purposes of this Schedule 7, "**Third Party Software**" means software which is proprietary to any third party which is or will be used by the Contractor for the purposes of providing the Services including the software specified in this Schedule 7. The Third Party Software shall consist of the following items:

Third Party Software	Supplier	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?

SCHEDULE 8 - SECURITY REQUIREMENTS, POLICY AND PLAN

INTERPRETATION AND DEFINITION

For the purposes of this Schedule 8, unless the context otherwise requires the following provisions shall have the meanings given to them below:

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

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

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

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

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

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

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

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

"Third Party Software" means software which is proprietary to any third party which is or will be used by the Contractor for the purposes of providing the Services including the software and which is specified as such in Schedule 6.

1. INTRODUCTION

This Schedule 8 covers:

1.1 principles of security for the Contractor System, derived from the Security Policy Framework, including without limitation principles of physical and information security;

1.2 wider aspects of security relating to the Services;

1.3 the creation of the Security Plan;

1.4 audit and testing of the Security Plan; and

1.5 breaches of security.

2. PRINCIPLES OF SECURITY

2.1 The Contractor acknowledges that the Authority places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Premises and the security for the Contractor System. The Contractor also acknowledges the confidentiality of Authority Data.

2.2 The Contractor shall be responsible for the security of the Contractor System and shall at all times provide a level of security which:

2.2.1 is in accordance with Good Industry Practice and Law;

2.2.2 complies with Security Policy Framework; and

2.2.3 meets any specific security threats to the Contractor System.

2.3 Without limiting paragraph 2.2, the Contractor shall at all times ensure that the level of security employed in the provision of the Services is appropriate to maintain the following at acceptable risk levels (to be defined by the Authority):

2.3.1 loss of integrity of Authority Data;

2.3.2 loss of confidentiality of Authority Data;

2.3.3 unauthorised access to, use of, or interference with Authority Data by any person or organisation;

2.3.4 unauthorised access to network elements, buildings, the Premises, and tools used by the Contractor in the provision of the Services;

2.3.5 use of the Contractor System or Services by any third party in order to gain unauthorised access to any computer resource or Authority Data; and

2.3.6 loss of availability of Authority Data due to any failure or compromise of the Services.

2.3.7 processing and storage of authority data within the UK or by exception within the EEA. Any processing outside of the UK must be subject to specific approval by the Authority.

3. SECURITY PLAN

3.1 The Contractor shall develop, implement and maintain a Security Plan to apply during the Contract Period (and after the end of the term as applicable) which will be approved by the Authority, tested, periodically updated and audited in accordance with this Schedule 8.

3.2 A draft Security Plan provided by the Contractor as part of its bid is set out herein.

3.3 Prior to the Commencement Date the Contractor will deliver to the Authority for approval the final Security Plan which will be based on the draft Security Plan set out herein.

3.4 If the Security Plan is approved by the Authority it will be adopted immediately. If the Security Plan is not approved by the Authority the Contractor shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit to the Authority for approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first

submission to the Authority. If the Authority does not approve the Security Plan following its resubmission, the matter will be resolved in accordance with clause I2 (Dispute Resolution). No approval to be given by the Authority pursuant to this paragraph 3.4 may be unreasonably withheld or delayed. However any failure to approve the Security Plan on the grounds that it does not comply with the requirements set out in paragraphs 3.1 to 3.4 shall be deemed to be reasonable.

3.5 The Security Plan will set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the Services and all processes associated with the delivery of the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with:

3.5.1 the provisions of this Schedule 8;

3.5.2 the provisions of Schedule 1 relating to security;

3.5.3 the Information Assurance Standards;

3.5.4 the data protection compliance guidance produced by the Authority;

3.5.5 the minimum set of security measures and standards required where the system will be handling Protectively Marked or sensitive information, as determined by the Security Policy Framework;

3.5.6 any other extant national information security requirements and guidance, as provided by the Authority's IT security officers; and

3.5.7 appropriate ICT standards for technical countermeasures which are included in the Contractor System.

3.6 The references to Quality Standards, guidance and policies set out in this Schedule shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such Quality Standards, guidance and policies, from time to time.

3.7 If there is any inconsistency in the provisions of the above standards, guidance and policies, the Contractor should notify the Authorised Representative of such inconsistency immediately upon becoming aware of the same, and the Authorised Representative shall, as soon as practicable, advise the Contractor which provision the Contractor shall be required to comply with.

3.8 The Security Plan will be structured in accordance with ISO/IEC27002 and ISO/IEC27001 or other equivalent policy or procedure, cross-referencing if necessary to other schedules of the Contract which cover specific areas included within that standard.

3.9 The Security Plan shall not reference any other documents which are not either in the possession of the Authority or otherwise specified in this Schedule 7.

4. AMENDMENT AND REVISION

4.1 The Security Plan will be fully reviewed and updated by the Contractor annually or from time to time to reflect:

4.1.1 emerging changes in Good Industry Practice;

4.1.2 any change or proposed change to the Contractor System, the Services and/or associated processes;

4.1.3 any new perceived or changed threats to the Contractor System;

4.1.4 changes to security policies introduced Government-wide or by the Authority; and/or

4.1.5 a reasonable request by the Authority.

4.2 The Contractor will provide the Authority with the results of such reviews as soon as reasonably practicable after their completion and amend the Security Plan at no additional cost to the Authority.

4.3 Any change or amendment which the Contractor proposes to make to the Security Plan (as a result of an Authority request or change to Schedule 1 or otherwise) shall be subject to a CCN and shall not be implemented until Approved.

5. AUDIT AND TESTING

5.1 The Contractor shall conduct tests of the processes and countermeasures contained in the Security Plan ("Security Tests") on an annual basis or as otherwise agreed by the Parties. The date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority.

5.2 The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. The Contractor shall provide the Authority with the results of such tests (in an Approved form) as soon as practicable after completion of each Security Test.

5.3 Without prejudice to any other right of audit or access granted to the Authority pursuant to the Contract, the Authority shall be entitled at any time and without giving notice to the Contractor to carry out such tests (including penetration tests) as it may deem necessary in relation to the Security Plan and the Contractor's compliance with and implementation of the Security Plan. The Authority may notify the Contractor of the results of such tests after completion of each such test. Security Tests shall be designed and implemented so as to minimise the impact on the delivery of the Services.

5.4 Where any Security Test carried out pursuant to paragraphs 5.2 or 5.3 reveals any actual or potential security failure or weaknesses, the Contractor shall promptly notify the Authority of any changes to the Security Plan (and the implementation thereof) which the Contractor proposes to make in order to correct such failure or weakness. Subject to Approval in accordance with paragraph 4.3, the Contractor shall implement such changes to the Security Plan in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the Security Plan to address a non-compliance with the Security Policy Framework or security requirements, the change to the Security Plan shall be at no additional cost to the Authority. For the purposes of this paragraph, a weakness means a vulnerability in security and a potential security failure means a possible breach of the Security Plan or security requirements.

6. BREACH OF SECURITY

6.1 Either Party shall notify the other immediately upon becoming aware of any Breach of Security including, but not limited to an actual, potential or attempted breach, or threat to, the Security Plan.

6.2 Upon becoming aware of any of the circumstances referred to in paragraph 6.1, the Contractor shall immediately take all reasonable steps necessary to:

6.2.1 remedy such breach or protect the Contractor System against any such potential or attempted breach or threat; and

6.2.2 prevent an equivalent breach in the future;

6.2.3 collect, preserve and protect all available audit data relating to the incident and make it available on request to the Authority;

6.2.4 investigate the incident and produce a detailed report for the Authority within 5 working days of the discovery of the incident.

6.3 Such steps shall include any action or changes reasonably required by the Authority. If such action is taken in response to a breach that is determined by the Authority acting reasonably not to be covered by the obligations of the Contractor under the Contract, then the Contractor shall be entitled to refer the matter to the CCN procedure set out in Schedule 3.

6.4 The Contractor shall as soon as reasonably practicable provide to the Authority full details (using such reporting mechanism as may be specified by the Authority from time to time) of such actual, potential or attempted breach and of the steps taken in respect thereof.

7. CONTRACT EXIT – SECURITY REQUIREMENTS

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

APPENDIX 1- OUTLINE SECURITY PLAN

SCHEDULE 9 – GUARANTEE (N/A)

SCHEDULE 10 - EXIT MANAGEMENT STRATEGY

Exit Management Strategy

See Page 9 in tender response

SCHEDULE 11 – KEY PERFORMANCE INDICATORS

CQC will appoint a nominated Contract Manager (or equivalent) who will oversee key performance indicators on a monthly basis with the contractor.
The contractor will be required to provide a meeting and activity reports to enable CQC to monitor:

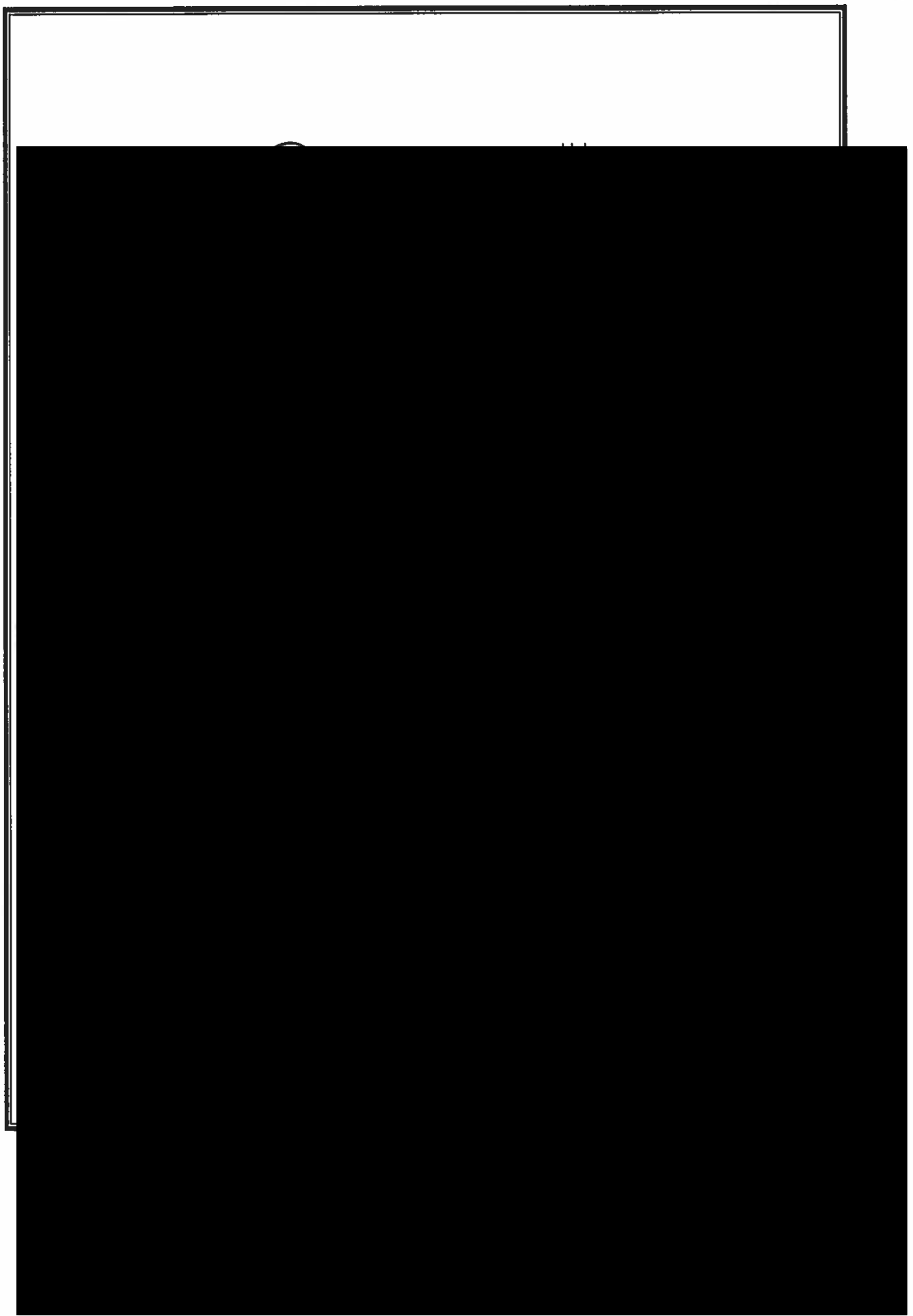
- Number of applications in progress at each stage of the DBS check
- Report on costs
- Progress in delivering the requirement:

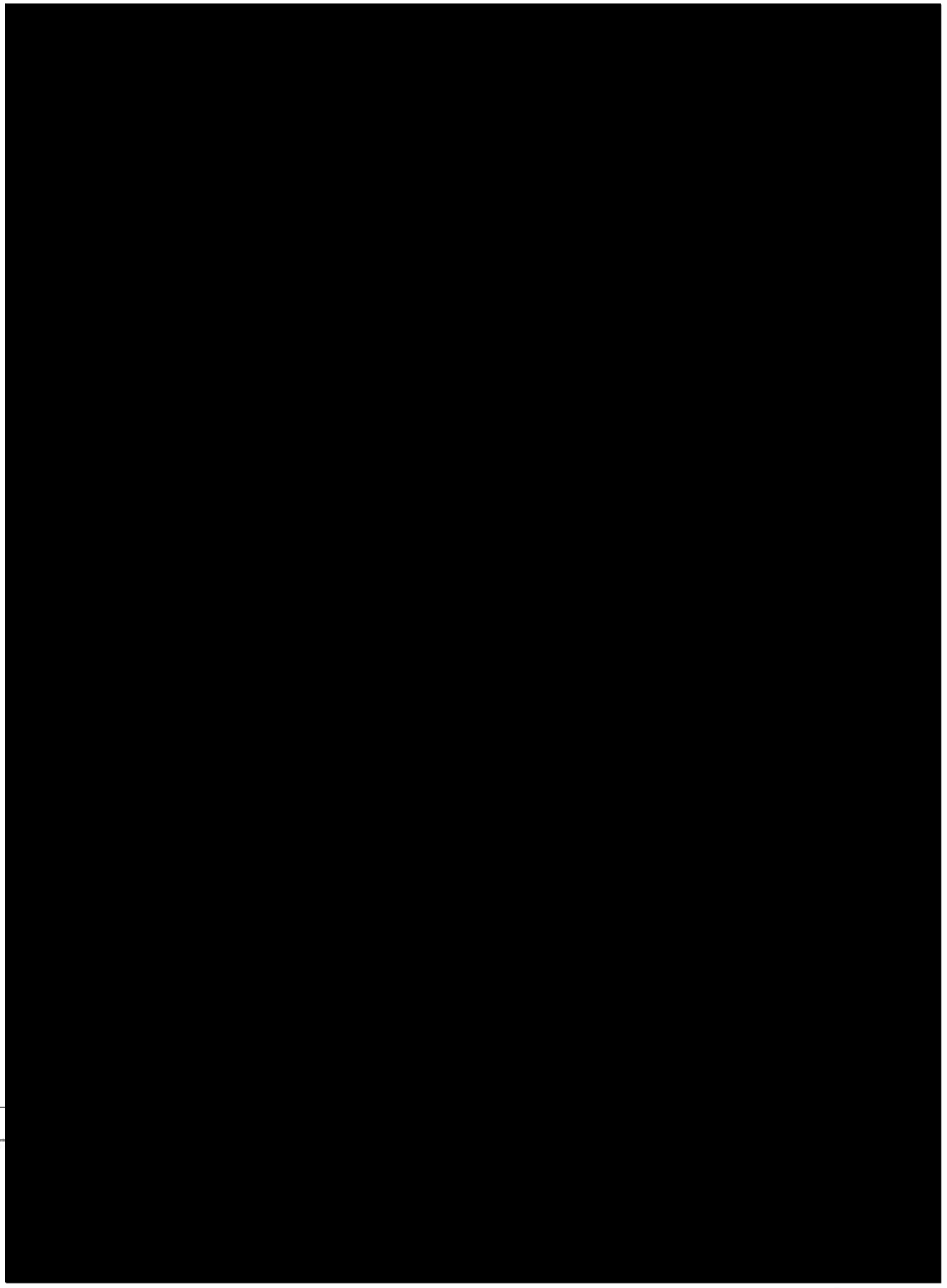
Key performance indicators will include:

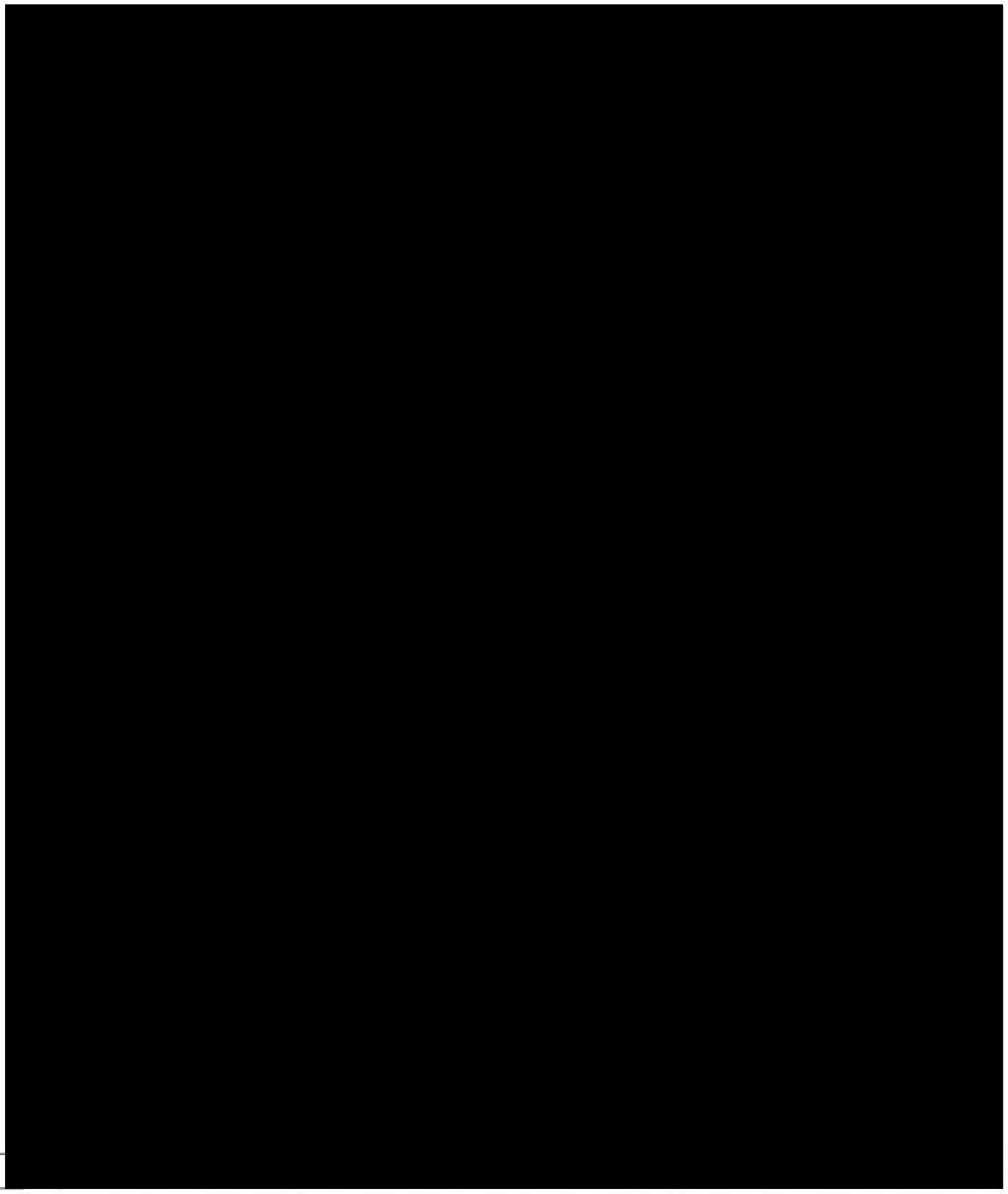
Key Performance Indicator (KPI)	Frequency	Threshold
Completed applications passed to DBS	As and When	3 days
Query response time frame (HR team)	As and when	2 days
Chase up outstanding DBS applications within their agreed SLAs	when identified	As defined by the Disclosure and Barring service time frames (after 60 days)
Update system in line with DBS information, in line with contract SLAs	as and when	Within 2 working days (or as jointly determined between CQC and the Supplier)
Add and remove new user accounts	As and When	2 working days
Respond to applicant queries	As and When	*2 working Days*

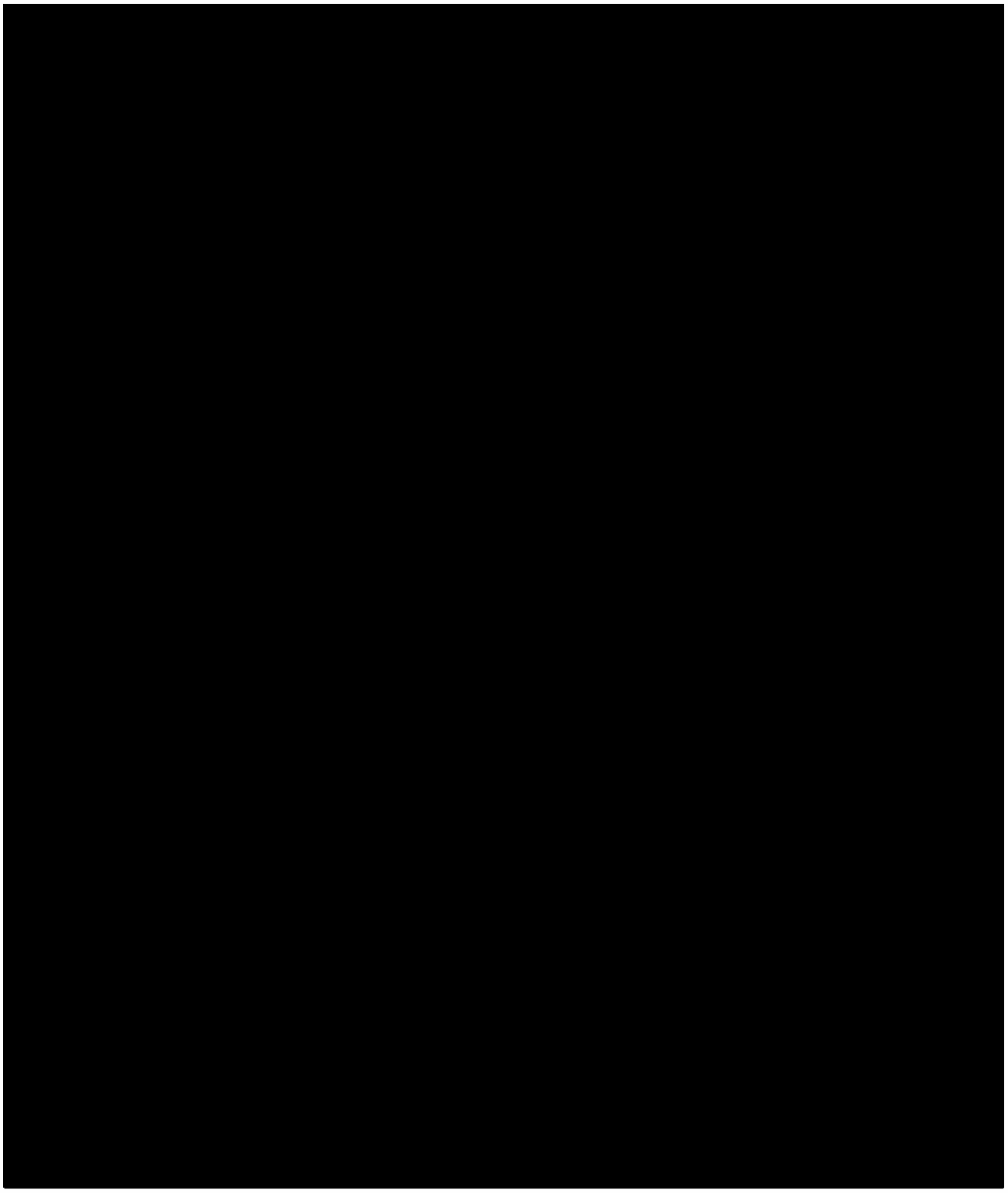
To monitor progress against the KPIs, the contractor must provide and agree the following with CQC:

Performing quality assurance on all aspects of the requirement;
- Provide CQC with timely and ongoing evaluation and quality assurance information relating to the service;
- Monitor the quality of the service provision to ensure customer satisfaction in accordance with the KPIs outlined in the Contract, unless otherwise approved by the Contract Manager;
- Attend a post contract review with CQC to review whether the objectives of the contract were met, to review the service and to identify any lessons learnt for future projects.









@lantic data ltd