CONTENTS

[1. PURPOSE 2](#_Toc444518866)

[2. BACKGROUND TO THE CONTRACTING aUTHORITY 2](#_Toc444518867)

[3. Background to requirement/OVERVIEW of requirement 2](#_Toc444518868)

[4. definitions 2](#_Toc444518869)

[5. scope of requirement 2](#_Toc444518870)

[6. The requirement 2](#_Toc444518871)

[7. key milestones 2](#_Toc444518872)

[8. authority’s responsibilities 3](#_Toc444518873)

[9. reporting 3](#_Toc444518874)

[10. volumes 3](#_Toc444518875)

[11. continuous improvement 3](#_Toc444518876)

[12. Sustainability 3](#_Toc444518877)

[13. quality 3](#_Toc444518878)

[14. PRICE 4](#_Toc444518879)

[15. STAFF AND CUSTOMER SERVICE 4](#_Toc444518880)

[16. service levels and performance 4](#_Toc444518881)

[17. Security requirements 5](#_Toc444518882)

[18. intellectual property rights (ipr) 5](#_Toc444518883)

[19. payment 5](#_Toc444518884)

[20. additional information 5](#_Toc444518885)

[21. Location 5](#_Toc444518886)

# PURPOSE

## The Annual Fraud Indicator values the collective loss to the UK economy from identified and hidden fraud at £193 billion per annum, with much of this being undetected.

## Fraud prevention is traditionally managed on a sector-by-sector basis; sharing data between public and private sectors in a consistent and structured manner has not been possible before.

## The Counter Fraud Data Alliance (CFDA) is a membership organisation for sharing data between organisations within the private and public sector for the prevention and detection of fraud, led by the Cabinet Office. The initial member organisations are:

* + - Cabinet Office (CO)
    - HM Revenue & Customs (HMRC)
    - Insurance Fraud Bureau (IFB)
    - UK Finance
    - Department for Work & Pensions (DWP)

## Further relevant member organisations may become members of CFDA in future (for example, local authorities, credit card agencies, credit rating agency, etc.). No formal agreements have been made at this stage.

## The data/information that shall be shared by members is that of covered individuals who are regarded as having committed fraud against their organisation and be referred to as ‘known fraudsters’. The Cabinet Office is seeking a specified anti-fraud organisation (SAFO), as provided for in section 68 of the Serious Crime Act 2007 and detailed within Appendix 1 of the ‘Data Sharing for the Prevention of Fraud,’ code of practice[1], to support the delivery of CFDA

# BACKGROUND TO THE CONTRACTING aUTHORITY

## The Fraud and Error (F&E) team within Cabinet Office have a responsibility to improve access to data and data analytics across government to counter fraud.

## It works with departments to:

* + - identify and reduce financial losses through fraud and error;
    - improve overdue debt management;
    - improve the effectiveness of grants whilst reducing the costs of their administration through the Grants Efficiency Programme;
    - identify more fraud and error and make sure changes are made to prevent it; and
    - provide counter-fraud remedies and common solutions to cross-cutting issues.

# Background to requirement/OVERVIEW of requirement

## The CFDA is a mechanism for sharing data between membership organisations within the private and public sector for the purpose of the prevention and detection of crime, specifically fraud. The data that shall be shared by members is that of subjects that are regarded as having committed fraud against their organisation and be referred to as ‘known fraudsters’. The system underpinning the CFDA should:

* + - Allow members to upload/provide their data to the CFDA Repository in a prescribed and secure manner.
    - Maintain the CFDA repository expressly for the use of, and purpose defined by, the CFDA members
    - Concatenate multiple source files into a single file for download by members.
    - Provide management information for the operators.

## Overall the purpose of the system is the prevention, detection and reduction of fraud.

# definitions

|  |  |
| --- | --- |
| **Expression or Acronym** | **Definition** |
| A&I | Analysis & Intelligence |
| Black data | Data and data sets of known fraud |
| CFDA | Counter Fraud Data Alliance |
| DWP | Department for Work and Pensions |
| F&E | Fraud & Error |
| FISS | Fraud Intelligence Sharing System |
| Grey data | Data and data sets of personal data where there is the suspicion of fraud |
| HMRC | Her Majesty’s Revenue and Customs |
| IFB | Insurance Fraud Bureau |
| IFR | Insurance Fraud Register |
| NCSC | National Cyber Security Centre |
| White data | Standard operational data and datasets |
| UKAS | United Kingdom Accreditation Service |

# scope of requirement

## The CFDA operating model is illustrated below:



## The successful Supplier will be required to establish the membership organisation of CFDA and to design, build, test/pilot, implement, operate, host

## The scope of the Supplier’s responsibilities will be structured into two phases as set out below, and described in more detail in section 6. It should be noted that the Cabinet Office and the CFDA Members will decide at the end of Phase 1 whether to proceed to Phase 2, depending on the outcomes and performance of Phase 1:

### During Phase 1: Design, Build & Implementation:

#### To set up the CFDA as a membership organisation, and to establish the structures of governance of the membership, in agreement with the Authority.

#### To design, develop (build, test and implement) the CFDA Repository, as illustrated in the Operating Model shown above, in compliance with the Authority’s requirements to support the membership (see section 6), with the customer interfaces and dependencies established as per the Draft Plan provided in the procurement process

#### To provide progress updates and attend governance bodies as required by the Authority, to support good governance and maximise the effectiveness of the CFDA.

### During Phase 2: Delivery:

#### To operate the CFDA as a membership organisation, supporting onboarding of members, adhering to the governance model, and providing ad hoc advice and support

#### To design, develop (build, test and implement) the CFDA Repository, as illustrated in the Operating Model shown above, in compliance with the Authority’s requirements to support the membership (see section 6), with the customer interfaces and dependencies established as per the Draft Plan provided in the procurement process.

#### To host the CFDA Repository in a suitably secure and reliable environment for the contract term.

#### To maintain the CFDA Repository such that it remains complaint with the Authority’s security requirements (see section 6).

#### To provide progress management information and attend governance bodies as required by the Authority.

## The scope of the CFDA Members’ responsibilities (i.e. not within the scope of requirement for the Supplier) will be:

### To build data extract mechanisms to create the necessary flat files for upload to the CFDA Repository.

### To build data download mechanisms to accept concatenated data files from the CFDA Repository.

### To build data import mechanisms to load data to their systems. These mechanisms may include filters to exclude records, or parts of records, that the member does not require.

### To participate in the CFDA governance and reporting structures.

# The requirement

## The requirement is to establish, under the auspices of a Specified Anti-Fraud Organisation, the operation of CFDA as a membership organisation for the Public Authorities, private sector organisations or associations as specified by the Contracting Authority, for sharing data between members for the prevention and detection of crime, specifically fraud The supplier will be required to put in place the appropriate structures to allow the membership organisation to operate. This includes working with CFDA Members to help them embed the operating model as widely as possible, facilitate the widest possible application of CFDA data and deliver the greatest benefits to the membership.

## The requirements for the CFDA Repository have been prioritised using the MoSCoW Scale:

### M - Must have this requirement to meet the business needs.

### S - Should have this requirement if possible, but project success does not rely on it.

### C - Could have this requirement if it does not affect anything else on the project.

### W - Would like to have this requirement later, but delivery won't be this time.

## Functional Requirements

| **No** | **Requirement** | **Priority** |
| --- | --- | --- |
|  | Allow CFDA members to upload a data file to the CFDA Repository via a secure file transfer mechanism, on demand.  NB. CFDA Members intend that upload will be via a system to system interface, however some members may require a manual upload and download process in the early stages of operation, with suitable access controls that comply with the Data Assurance requirements. There is an expectation of two factor authentication in such cases. | M |
|  | Maintain the CFDA repository in isolation, expressly for the use of, and purpose defined by, the CFDA Members | M |
|  | Perform simple validation to verify that:   * the uploaded file has not become corrupted in transit; and * all mandatory fields are populated, including appropriate field validation.   NB. Detailed validation of file contents is out of scope for the Supplier. Responsibility for data quality sits with the CFDA Members. | M |
|  | Notify the member of the outcome of the upload (i.e. success or failure) with any rectification requirements.  NB. It will be the responsibility of the CFDA Member to detect that a file has failed validation and resubmit. | M |
|  | After each successful upload, replace or increment the previously uploaded member file with the newly uploaded file such that only one file per member is held at any one time.  *NB. ‘Replace’ implies a bulk upload every time; ‘’increment; implies uploading ‘delta’ files. Potential Providers are asked to recommend the most efficient and cost-effective approach given the potential for a large increase in the number of members.* | M |
|  | Members will be able to flag a record for deletion e.g. in the event that a previously notified ‘known fraudster’ no longer meets the criteria and should therefore be removed from CFDA.  *NB. This applies primarily to incremental upload. Bulk upload each time would mean the removed record would no longer appear. In this case, members would still need to spot the removal at the next download.* | M |
|  | Concatenate all uploaded files to create a single file.  NB. Records within the uploaded files will be tagged by the member that provided that data, so the order of concatenation is unimportant.  *Potential Providers are asked to propose the most cost effective and efficient mechanism to satisfy this requirement. For example, rebuilding the concatenation every time there is a successful upload or waiting until all expected files have been received. The mechanism must be suitable for the initial four members and be scalable for a much larger group of up to 500 members.* | M |
|  | Notify CFDA members when a new concatenated file is ready for download. | M |
|  | Allow members to download a concatenated data file from the CFDA Repository via a secure download mechanism, on demand. | M |
|  | Allow CFDA Members to withdraw an uploaded data file, on demand.  *NB. The Authority recognises that this requirement has implications for data retention: i.e. should the previous file be retained and reinstated if a file is withdrawn. The Supplier is expected to resolve this during detailed design.* | M |
|  | Provide management information to CFDA Members on demand for a user-defined period.  NB. Detailed requirements will be agreed during the design and build phase, but are expected to include but not be limited to:   * Number of uploads and downloads (total, by each member etc.) * Number of records uploaded and downloaded (total, by each member etc.) * System performance (e.g. availability, number of outages, time to restore service etc.) | M |
|  | Provide alerts to CFDA Members if usage (i.e. uploads or downloads) exceeds a user-defined threshold to be agreed with members during the detailed design phase. | M |

## Non-Functional Requirements

| **No** | **Requirement** | **Priority** |
| --- | --- | --- |
|  | Recovery time objective:  In the event of a system outage, recover the system to full operational status within two working days.  For example:   * Failure at 1000 Monday; recover by 1000 Wednesday * Failure at 1400 Friday; recover by 1400 The following Tuesday (or Wednesday if Monday is a Bank Holiday) | M |
|  | Recovery point objective:   * No more than 24 hours’ worth of data shall be lost i.e. data files uploaded more than 24 hours prior to the outage shall be recoverable. | M |
|  | Scalability objective:   * Ensure that the service is scalable, in line with the projected volume increases for the first 3 years as a minimum. | M |
|  | Members shall be alerted to an outage:   * Within two hours of occurrence. * Within two hours of restoration so that they can manually resubmit if necessary. | M |

## Data Assurance Requirements

| **No** | **Requirement** | **Priority** |
| --- | --- | --- |
|  | The Supplier's solution shall be ISO27001:2013 certified (by a UKAS accredited certification body) and shall be Cyber Essential Plus certified or be willing to obtain these certifications within an agreed timescale as per the Security Schedule. | M |
|  | The CFDA Repository data shall be hosted, stored and processed within the UK.  For the avoidance of doubt, this requirement applies to the live data and any backups. | M |
|  | Maintain a searchable audit log of activity on the CFDA Repository, including but not limited to:   1. Uploads (date/time, source etc.) 2. Number of records uploaded in each file by each CFDA Member 3. Failed uploads (date/time, source etc.) 4. Withdrawn uploads (date/time, source etc.) 5. Downloads (date/time, source etc.) | M |
|  | The Supplier must ensure an effective protective monitoring regime is in place at all times and produce sufficient evidence in the form of logs and   other documents to the Authority to confirm this. The Supplier should:   1. Provide operational security management reports. 2. Engage with the Authority incident management process. 3. Demonstrate the ability to deliver protective monitoring across the supply chain 4. Incorporate National Cyber Security Centre (NCSC) guidance on how to design a security operations centre ([SOC](https://urldefense.proofpoint.com/v2/url?u=https-3A__www.ncsc.gov.uk_guidance_security-2Doperations-2Dcentre-2Dsoc-2Dbuyers-2Dguide&d=DwMFaQ&c=cUkzcZGZt-E3UgRE832-4A&r=ckcPamptTkUeQLipUvrAVv7P9w_f1qf8dQlQtr-oE8o&m=sx5oAhCeHg2V07q1Sf5Mvtn_rAp1Oh4PmhGivoRSXyw&s=DWTsii_DN9hXCCQyM5zKdZkAsGRrnkKpE5Vj2MUWL4w&e=)). | M |
|  | All Supplier staff which have access to Authority/Buyer data must be willing to undergo security clearances and this will be mandatory for any staff accessing bulk data. As a minimum, all staff must comply with the Baseline Personnel Security Standard.  Supplier staff who will have access to bulk live data (classified as Official Sensitive data) must be willing to undergo an elevated clearance level (SC). Further information on the types of security clearance can be found here: <https://www.gov.uk/government/publications/hmg-personnel-security-controls> | M |
|  | The supplier shall ensure that no access to system is possible via mobile devices. | M |
|  | Raw data shall be held on fixed systems i.e. not mobile devices, laptops etc. | M |
|  | CFDA Members cannot amend other member data sets. | M |
|  | Files shall be encrypted at rest and on the move to the appropriate Government standard. | M |
|  | Public cloud hosting shall not be used for the CFDA Repository. | M |

## Member Functions (i.e. not a requirement of the CFDA Repository Supplier and included only for completeness)

| **No** | **Requirement** | **Priority** |
| --- | --- | --- |
|  | Members to carry out the necessary data preparation prior to upload. | M |
|  | Data to be transferred using flat files; the type should be open to accommodate member wishes. | M |
|  | Header and footer file details to be generated to include details of file. | M |
|  | Validation at the point of the upload/download will be carried out by the Member. | M |
|  | If laptops are used to hold CFDA data then they shall be encrypted. | M |

# key milestones

## The Potential Provider should note the following project milestones that the Authority will measure the quality of delivery against:

|  |  |  |
| --- | --- | --- |
| **Milestone** | **Description** | **Timeframe** |
| 1 | Detailed Plan for Delivery based on the draft plan submitted as part of the procurement process, and reviewed with the Authority at contract start. The Draft Plan and the Detailed Plan should include the final TOM, dependancies and interfaces with the Authority and other customers | Within week 1 of Contract Award |
| 2 | Detailed Requirements | Within week 2 of Contract Award |
| 3 | Draft Detailed Solution Design provided in Week 3 for discussion with the Authority and Agreement by Week 4 | Within week 4 of Contract Award |
| 4 | Solution Build & Test against the criteria and processes set out by the Authority | Within week 6 of Contract Award |
| 5 | Solution Implementation, go-live & Stakeholder Acceptance against the critieria set out by the authority. For the avoidance of doubt, Acceptance will include all operating manuals, system hanover, and so on that enable the Authority (or appointed contractor) to take over the running of the system if requiredNB. Achieving this milestone marks the end of Phase 1. At this point the Authority, in consultation with CFDA Members, will decide whether to proceed to Phase 2 under this Contract | By 31 March 2018 |

# authority’s responsibilities

## Cabinet Office as contracting authority will take the role of Lead Client and will::

### Manage and oversee the delivery by the supplier of Phase 1 of the project on behalf of the CFDA Members (also known as users or customers).

### Co-ordinate weekly team meetings between the Client and the Supplier to monitor progress during Phase 1 and the early stages of Phase 2 (at least the first three months) to address any problems and adjustments. Thereafter responsibility for co-ordinating service performance meetings, on at least a monthly basis, transfers to the Supplier.

### Act as escalation point to deal with issues, for example if a CFDA Member is not fulfilling its responsibilities in a timely or effective manner as described in the governance model.

### Manage and oversee the provision by the supplier to the membership of: the membership services, operational management and continuous improvement during Phase 2.

## Each CFDA Member will:

### Nominate a single point of contact to be available to the Supplier throughout the project to act as a “key customer” focal point. Support and attend governance meetings Provide access to staff with relevant expertise in a timely manner to support the project e.g. detailed requirements, development and test.

### Provide access to staff with relevant expertise in a timely manner -to support the project e.g. detailed requirements, development and test, as set out in the Draft Plan and the subsequent Detailed Plan

### Provide test data files, in either the current agreed format or to a format agreed with the supplier, containing synthesised or anonymised data to support development and test..

### Construct the necessary extract, upload, download and import mechanisms to support development and test.

### Provide feedback on draft deliverables within a reasonable period of time.

### Undertake the provision of data on an ongoing basis throughout Phase 2.

# reporting

## The Supplier’s reporting responsibilities are as follows:

### During Phase 1: Design, Build & Implementation:

#### Weekly highlight reports documenting progress against plan, risks and issues etc.and any rectification proposals against any issues utilising exception request in pre-agreed formats.

### During Phase 2: Service Delivery:

#### Monthly status reports documenting the solution performance as well as use of and access to the system.

#### Supporting and servicing ongoing governance of the CFDA membership organisation, including but not limited to support to growth and onboarding plans.

# volumes

## The volume of data that the CFDA Repository is required to hold is not large. The predicted data volumes at go-live are estimated as:

|  |  |  |  |
| --- | --- | --- | --- |
| **Member** | **Weekly** | **Monthly** | **3 years Initial upload** |
| **DWP** | 4,769 Rows | 20666 rows | 744,000 rows |
| **HMRC** | 4,769 Rows | 20666 rows | 744,000 rows |
| **IFB** | Est. 500 rows | Est.2000 rows | 36,000 rows |
| **UK Finance** | 559 rows | 2422 rows | 106452 rows |

These numbers are indicative and subject to change

## Potential Providers should note that the volumes of data to be stored are of the order of MB or GB and not TB and should scale the CFDA accordingly. Nevertheless, the infrastructure should be scalable as a minimum to meet the first three year forecast to allow for additional data points and not require a rebuild, and thereafter under change control.

# continuous improvement

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

## The Supplier should present new ways of working including continuous improvement proposals to the Authority during Contract review meetings, at least on a quarterly basis, with justification for any change proposed.

## Changes to the way in which the Services are to be delivered must be brought to the Authority’s attention and agreed prior to any changes being implemented and be taken through the established change control process.

# Sustainability

## Not applicable.

# quality

## Potential Providers must be accredited to:

### ISO27001/2 or equivalent.

### ISO9001: 2015 or equivalent.

# PRICE

## Potential Providers are required to provide:

### A firm price for Phase 1: Design, Build, Test & Implementation. The price should be broken into components linked to major deliverables as set out in section 6 and the Draft Plan. Prices are expected to be competitive, reasonable and not in excess of £350k.

### A firm estimate for Phase 2: Service Delivery, with a clear set of financial and other assumptions, milestones outcomes, and dependencies. Prices are expected to be competitive, reasonable and not in excess of £104k in total per annum. They should include:

#### Annual hosting for the full term; and

#### Discounts on hosting costs e.g. if the Authority were to commit for longer than one year at a time.

### A firm estimate to cover the costs of Test, Implementation and any operational cost for a new member of CFDA, with clear financial and other assumptions and dependencies.

### NB. The Authority’s requirement is that the solution is designed to be scalable from the outset such that the additional members and data can be accommodated without system rebuild.

### A rate card for maintenance and development against the categories set out in the pricing template

### The Authority is interested in any variant pricing e.g. risk/reward mechanisms. A variant pricing offer must accompany compliant pricing to be considered. Any variant must be fully explained and priced in order to enable a full evaluation, including but not limited to assumptions on ability to accelerate growth of the CFDA, key data, benefits and risks, Authority responsiblities and overall value for money.

## Prices are to be submitted via the Appendix E excluding VAT. Variant pricing models should follow Appendix E as closely as possible.

# STAFF AND CUSTOMER SERVICE

## The Authority requires the Potential Provider to provide a sufficient level of resource throughout the duration of the CFDA Repository Contract in order to consistently deliver a quality service to all Parties which meets the expectation and requirements of the contract.

## Potential Provider’s staff assigned to the CFDA Repository Contract shall have the relevant qualifications and experience to deliver the Contract, as set out in the Draft Plan and Final Plan.

## The Potential Provider shall ensure that staff understand and uphold the Authority’s vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.

# service levels and performance

## Service Levels are defined in section 6 above.

## Remedies for poor performance will be in accordance with the terms and conditions.

# Security requirements

## Security requirements are documented in section 6 above.

# intellectual property rights (ipr)

## All IPR will be owned by Cabinet Office.

# payment

## Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

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

# additional information

## Not applicable.

# Location

## The location of the Services will be carried out at the Supplier’s premises, with occasional visits to Cabinet Office and to CFDA Members’ offices in London.