ISO 27001:2013 Certification Tender Requirements

**High-level Requirement**

We are looking for a UKAS accredited organisation to deliver ongoing ISO 27001 assessment and certification. This will involve transfer of our current certificate.

**Overview**

Companies House (CH) is an Executive Agency of the Department of Business, Energy and Industrial Strategy (BEIS). As of the 1st April 2020 Companies House will change status from a public corporation to central government.

The main functions of Companies House are:

* Incorporate and dissolve limited companies.
* Examine and store company information delivered under the Companies Act and related legislation.
* Make this information available to the public,

Companies House employs around 1100 people of which the majority are based in Cardiff.  All document processing for English and Welsh companies are performed at the Cardiff office.  The equivalent for Scottish companies is administered at the CH Edinburgh office (around 25 staff). The equivalent for Northern Irish companies is administered at the CH Belfast office (around 20 staff). In addition to these offices, CH has an information centre in London (around 8 staff).

**Current ISO 270001 status**

Companies House was first attained certification ISO27001 in 2005 and is currently certified to ISO27001:2013. Certification has been maintained throughout this period.

**Scope of current certification**

The scope of the current certification is:

*The Information Security Management System (ISMS) supporting the activities of the IT department of Companies House in the central provision of IT to the organisation and the specific business processes of the Companies House e-Business systems. This includes the provision of electronic filing of statutory company documents and the publication / provision*

*of this information to the public via online services.*

**Requirements**

* The tendering organisation *must* be UKAS accredited to provide certification to Information Security Management Systems ISO 27001:2013.
* The successful bidder *must* arrange for the transfer of our existing ISO 27001:2013 certification from the current accredited organisation
* This transfer *must* be completed by June 2020
* The successful bidder *must* deliver ongoing assessment and certification of our ISMS in line with ISO 27001:2013 requirements
* The first surveillance visit *must* be carried out in September 2020
* Further surveillance visits must be carried out in March and September for the duration of the contract
* Our first preference is for surveillance visits and certification activities to be carried out at our Cardiff office; however it may be necessary to hold these visits remotely.
* Prior to the award of the contract, the proposed auditor who will be carrying out the surveillance visits and certification activities, must attend a meeting remotely.
* The proposed auditor should undertake all surveillance visits and certification activities throughout the duration of the contract
* Where this is not possible, the successful bidder must arrange a formal handover to a new auditor. This should include a meeting with them remotely or at Companies House.
* We require at least 4 months’ notice for the date of the next visit.
* If any visit needs to be cancelled a two-week cancellation notice period is required. What is the contingency plan is for any cancelled visit?

**Information required**

* We require the following information:
  + How your organisation meets our requirements including:
    - The process for transferring of our certificate from our current certification organisation to yours.
    - Your organisation’s approach to the assessment and certification process. This should include the structure of the surveillance visits, certificate renewal, number of days required for each assessment and the process for managing any non-conformities found.
    - The ability of your organisation to meet schedule for our surveillance and certification visits.
    - The day rate should any additional audit days be required.
    - The ability of your organisation to deal with cancellation in line with our requirements above.
    - The ability of your organisation to carry out the certificate transfer, surveillance visits and certificate renewal remotely.

**Deliverables**

* Surveillance and certification visits carried out in line with UKAS and ISO 27001:2013 requirements
* All surveillance and certification visits carried out at our Cardiff office or remotely.
* Schedule of surveillance and certification visits, in line with the timeline below, for the duration of the contract.

**Evaluation**

* How many years’ experience does the organisation have in certifying to ISO 27001:2013? – 15%
* How many government organisations does the auditor have experience with in delivering ISO 27001 audits? – 30%
* Can the organisation carry out surveillance visits and certification activities remotely – 10%
* What is the approach to delivery of surveillance certification visits in? – 20%
* Price – 25%

**Timeline**

* Meet auditor via remote meeting w/c 18th May or w/c 26th May 2020.
* Certificate transfer to start on 1st June 2020 and be completed by 30th June 2020
* The next surveillance visits to take place in September 2020
* Six-monthly surveillance visits in March and September during the period of the contract.
* Our certificate expiry is the 2nd March 2023. The re-certification audit must take place in line with any ISO 27001 requirements to give Companies House the allowed time to rectify any non-conformities to ensure continuation of our certification.

**Duration of contract**

Three years plus one-year extension if required