Clarification Questions and Responses

Companies House Iso27001 Certification

Commericial Lead: Carlson Charles

2020

Please see below all clarification questions that have been received before the clarification deadline and their responses below. This is being circulated to all bidders. **The deadline for all final bid submissions is the 28th of April 2020 at 12pm noon.** **Any bids received after this time may not be considered. All submissions should be submitted to the following email** [**Ccharles@companieshouse.gov.uk**](mailto:Ccharles@companieshouse.gov.uk)**.**

The bid clarification questions and answers are as follows:

**Question 1: Number and types of operating systems (Mac, Linux, Windows etc)?**

* Oracle Solaris & RedHat Linux for Line of Business apps
* MS Windows & Novell OES for Back Office
* MS Windows & MacOS for desktops/laptops

**Question 2: Number of internal servers and or NAS storage devices?**

* Circa 650 (including physical and virtual) between on-premise and DR data centres. Circa 600 in the Cloud.
* 3 SANs

**Question 3: Number of databases?**

* Around 10 core databases plus many dev and test
* Mainly Oracle

**Question 4: Number of segregated networks?**

* Three

**Question 5: Number of key applications?**

* Around 10

**Question 6: Number of staff per location?**

* Cardiff – 1,000
* Edinburgh – 38
* Belfast - 16
* London - 8

(Edinburgh, Belfast and London are not currently in scope of our certification)

**Question 7: Ideally, to propose a transfer of ISO27001 certification, the existing certificate must be in force, within the validity period, ideally, please can you provide a copy of your current certificate and the most recent assessment report?**

* The existing certificate is in force and expires March 2023.

**Question 8: Can you confirm that there are no major non-conformities currently across the scheme?**

* There are no major non-conformities across the scheme

**Question 9: What is the business need driving this tender activity?**

* We have been certified for 15 years and see ISO27001 as a requirement to ensure we have controls in place to protect the CIA of our information.

**Question 10: Has the organisation had any reportable information security incidents(for example security breaches) that must be reported / have been reported to a regulator at any of the sites to be included in certification within the past 24 month period?**

* Yes

**Question 11: Has the organisation had any pending (or completed in the last 24 months) legal actions concerning information security management?**

* No

**Question12: Bring your own device (BYOD) policy is permitted by our organisation?**

* BYOD is not allowed

**Question 13: Our organisation conducts system develops activities either in-house or outsourced (e.g. software/hardware development)?**

* Development is in house, but we do manage 3rd party scrums in house.

**Question 14: If the information produced by our product/service is incorrect or incomplete there is a threat to individual or collective health/well being/safety/security/miscarriage of justice or risk of fraud?**

* Yes

**Question 15: Does Companies House shares sensitive information with third parties?**

* Customers'/end users'/staff or others personal information .e.g. outsourced payroll, third party vetting services (criminal records, credit checks)
  + Yes
* Intellectual property (designs, source code or other sensitive proprietary information)
  + Yes (but very limited)

**Question 16: Is the ISO 27001 system integrated with any other management system that you are certified to – ISO 9001 for example?**

* No.

**Question17: Are the functions performed in each of the other sites the same as those carried out in the Head office.  If not what functions are in each site?**

* The scope is just the Cardiff site.

**Question 18: What stage of the certification cycle are in at the moment – Surveillance 1, 2, or recertification?**

* Surveillance 1

**Question 19: Is six monthly the preferred audit cycle or do you wish to move to an annual cycle?**

* 6 monthly

**Question 20: Do you have any Non Conformities outstanding from your last audit?  If so how many and do you plan to close them before with your current CB?**

* 3 minor non-conformities.  They will be closed by the successful organisation

**Question 21: Do you have roles within your organisation that are repetitive?  E.g. 500 staff perform exactly the same function.**

* Yes

**Question 22: In relation to IT specifically, what is the extent of your and diversity of technology utilised?**

* Standardised but diverse IT platforms, servers, databases, networks etc

**Question 23: How would you assess the risk?**

* High regulatory requirements

**Question 24: What as an organisation do you outsource and how dependent are you on the outsourced arrangements?**

* The Contact Centre is outsourced.   Elements of IT Development are outsourced to third parties but managed internally.  We are increasingly using IaaS to deliver our services and SaaS to support the business

**Question 25: Do you have or do any in house software development and if so what is it?**

* As above.

**Question26: Please provide current schedule of audits across the cycle up to recertification in 2023.**

* As per our requirements document we require 2 x surveillance visits per year and 3 yearly re-certification audit