# Social Work England 00336 – Response to Clarification Questions

Q) How many web applications would be in-scope, as the document appears to address multiples – CRM, Extranet and internally developed applications. Would you be able to provide more detail around the functionality, and typical user roles per application? **A) Social Work England have a public facing website (Umbraco), and a CMS (Appian) used by both our internal users (standard user or administrator), and our external clients (Social Workers).**

Q)With regards to the internal infrastructure assessment a) How many IP addresses would be in-scope? b) Are any system build reviews (authenticated check of configuration) required? c) Are any system build reviews (authenticated check of configuration) required? d) Wireless networks are mentioned, how many wireless networks and access points are in-scope? **A) – a) As the majority of Social Work England’s Employees are currently working remotely, this figure is in the early twenties. Although when the main office is at its usual capacity, this figure is usually circa two hundred. b) No. c) No. d)** **There are two x SSID’s, and fourteen x Access Points**

Q) How many Azure / O365 Tenancies would be in-scope for testing? A) – **Two Tenancies would be in scope.**

Q) **Regarding Web Application Penetration Testing** – a) How many web Sites/URLs to be tested? b) How many static pages are there?  c)  How many dynamic pages d) Is the test authenticated or unauthenticated?  e) How many user levels in the authentication page?   **A) – a) One b) Fifty + c) Fifty + d) Both authenticated & unauthenticated e) Four +**

Q)- Can the internal test be performed from one site rather than going to another site? (can we access other office's network from single office) **A) There is only one site.**

Q) **Around Wireless Penetration Testing** – a) How many SSIDs? b) How many sites to be tested?  **A) – a) Two b) One**

Q) **Regarding O365/Azure Auditing** - How many Tenants and Subscriptions? – **A) There are 2 x Tenants - 205x M365 E5, 210x M365 F3.**

Q) Can testing be carried out during normal working hours? **A) Yes**

Q) Please confirm Web application name(s) and URL(s) **A)** **socialworkengland.org.uk**

Q)How many applications are in scope of the assessment? **A) 3**

Q) Does the application require authentication? If so, how many user levels are there? **A) 4**

Q) Does the application or service store or process sensitive information such as medical, financial, corporate-confidential, or personally identifying details?  **A) Yes**

Q)Does your application or service have any regulatory requirements, such as PCI DSS (for credit and debit card data?)**A) No**

Q) Is the web application based on an off-the-shelf CMS or application?  **A) No**

Q)Can users register their own accounts?  **A) Yes**

Q)How many functions does your web application have? **A) 50+**

Q) How many directly editable input fields, such as “name” or “account number”, does your web application have**? A) 200+**

Q) How many workflows does your web application have? **A) 30+**

Q)What is the approximate number of unique pages (both static and dynamic) within the application? **A) 100+**

Q) How many databases require assessment (if any)? **A) 3**

Q)How many IP subnets or VLANs are in scope? **A) 4 Subnets**

Q) How many live IPs per subnet are in scope? **A) Due to the ongoing COVID-19 pandemic, there are limited numbers = x 12, usually, and x 200 in total across all subnets.**

Q) How many servers are in place which require review and what are their operating systems? -**A) N/A**

Q) Can any documentation or network diagrams be shared at this stage?  **A) No**

Q) Is authenticated user testing required? **A) Yes**

Q) How many firewalls require assessment? **A) 1 (we have 2 in HA)**

Q) How many firewall rules does each have? **A) 45 – not all in use**

Q) How many SSIDs are in scope for the wireless assessment? How many Access Points? A) **2 x SSIDs & 14 x AP’S**

Q) How many VPNs for remote access require assessment? **A) None**

Q) How many remote access gateways are in scope? **A) None**

Q) **Web Application** – Can the authority give us an idea of size of the web application to be pentested. To include the number of rolls and pages? **A) There are 1 x URL, 50+ functions, 200+ fields, 100+ pages & 4+ user levels.**

Q) **Network Infrastructure** – Is this an internal pentesting requirement, or external pentesting requirement or both? In each case please can you provide the number of IPS to be tested against? **A) Both requirements are covered. There are 2 public IP’s, usually 200+ internal IP’s over 4 subnets. However due to the COVID-19 Pandemic, this is minimal.**

Q) **O365/ Azure** – Can you given us further details of the size of the application within the organisation to be pentested please as there is currently no detail with in the ITT **A) There are 2 tenants - Main: ~200 users, ~200 guests, ~200 devices, ~250 mailboxes, ~230 SharePoint Sites, Multiple Config policies, conditional access policies, enterprise apps, SSO enabled. 2nd tenant: ~200 users/mailboxes, ~10 SharePoint sites, minimal policies**

Q) How many web Sites/URLs to be tested? **A) One**

Q) How many static pages**?  A) Fifty**

Q)How many dynamic pages? **A) Fifty**

Q) Is the test authenticated or unauthenticated?  **A) Both**

Q)How many user levels in the authentication page?  **A) Four +**

Q) How many hosts/IP's to be tested (INTERNAL) **A) As Social Work England’s employees are currently working remotely in the main, we currently have circa x 20. When the office is at full capacity, we have circa x 200**

Q) Can the internal test be performed from one site rather than going to another site? (can we access other office's network from single office) **A) There is only one site.**

Q) How many SSIDs? -**A) Two**

Q) How many sites to be tested?  **A) One**

Q) O365/Azure Auditing: How many Tenants and Subscriptions? **A) 2 Tenants - 205x M365 E5, 210x M365 F3**

Q) Is it acceptable if we submit a joint bid with a partner, as the partner has all the necessary accreditations and experience to deliver the testing? **A) Although Potential Providers are able to provide the Services in collaboration with a partner, Social Work England's preference is to work directly with an organisation (without any sub-contracting relationship). All compliant tender submissions received will be evaluated, however, a consideration of the delivery method will be made when scoring submissions.**

Q) What does the web application do? **A) Social Work England’s Web application is Appian. This application is used for our CMS system and accessed by users internally, and also by our client base externally.**

Q) How is the application hosted? – **A) The application is hosted on AWS VM’s.**

Q)How many Functions does the application have? - **Fifty +**

Q)How many user levels does the application have? **A) Four +**

Q) How many pages? Dynamic / Static **A) One Hundred +**

Q)How many input fields? **A) Two Hundred +**

**Web Services (API’s)**

Q) Number of API’s: **Fifty +**

Q) Number of Methods/Calls per API **A) The numbers around this are difficult for Social Work England to quantify. Several them are used with every transaction.**

Q) Number of parameters per Method/Call **A) Between two & ten.**

**O365 Audit\Azure Penetration Test:**

Q) Number of Users **A) Tenant 1 has: 210 Members- 200 Guests. Tenant 2 has: 210 Members ~20 guests.**

Q) Number of Servers **A) N/A**

**Any related infrastructure that needs testing**

Q) IP’s: **A) As the majority of Social Work England’s employees are currently working remotely, this figure is lower – circa 20. This number is usually ~200 - 2 public IP’s.**

Q)Firewalls (Model and number of rules) **A) PA 3060, 45 rules Q) Number of Servers (Operating system): N/A**

Q) Databases (Number and Type) **A) Only as part of Web app hosted virtually in AWS & Azure.**

**How many web applications would be in-scope, as the document appears to address multiples – CRM, Extranet and internally developed applications.**

Q) Would you be able to provide more detail around the functionality; and typical user roles per application **A)** **We have public facing website (Umbraco), and a CMS (Appian) used by our internal users (standard user or administrator) and also our external clients (Social Workers)**

**With regards to the internal infrastructure assessment.**

Q)How IP addresses would be in-scope? **A) As currently homeworking not many, a couple of dozen. Usually nearly 200.**

Q) Are any system build reviews (authenticated check of configuration) required? **A) No**

Q) Are any firewall/network device configuration reviews required? **A) No**

Q)Wireless networks are mentioned, how many wireless networks and access points are in-scope? **A) Two SSIDs, 14 Aps**

Q) How many Azure/O365 Tenancies would be in-scope for testing? **A) Two**

Q) Can you confirm if there are any API’s contained within the Umbraco website or Appian CMS, if so, can you confirm the number of methods and roughly number of parameters per method? **A) 50+ API’s, we don’t know the exact number of methods, but approx. 2-10 parameters per call**

Q)Can you provide a brief description of the Appian CMS? - **Appian CMS is the main system used internally by employees and also by our client base – aka Social Workers, to register and upload CPD. Main functions: logging in, uploading docs, etc 50+ functions, Number of pages = 100+**

Q) Could you provide a rough number of workstations in scope for the internal infrastructure assessment? - **This can be dependent on the day of the week, due to the ongoing COVID-19 Pandemic. We could be closed, or we could have up to a dozen devices.**

Q) Could you provide a rough number of servers in scope for the internal infrastructure assessment? **A) There are None.**

Q) Can you confirm if a network device review e.g. firewall rule review is required? If so, can you please provide a breakdown of the make and model of each device in scope **A) Palo Alto 3060**

Q) Can you confirm if external penetration testing of the external IP address ranges of SWE is required? **A) Yes, we have two public IP’s.**

Q) Could you provide any high-level diagrams of the Azure/O365 tenancies, if not could you provide further detail about each tenancy? i.e. number of v-nets, servers, virtual machines etc **A) Azure AD is very limited currently, only SSO and enterprise apps in use. O365 includes, 200 users, 300 mailboxes, 200 guests, 100+ groups, config policies, compliance policies, security policies (all numbers circa)**

Q)  Can you confirm if there is a requirement for any server build reviews within the Azure tenancies? **A) N/A**

Q) Is there a particular standard or industry best practice you want the Azure tenancies to be reviewed against? **A) No, there are no particular standards/industry best practice, to review the tenancies against.**

Q) Can you confirm if SWE is interested in Social Engineering Exercises such as, phishing campaigns and physical social engineering engagements? **A)** **Not at this time, no.**

Q) Since it is a 2 years contract are we taking in consideration the scope to be the the current number of assets 20 or the overall count 200? **A) If these users still connect to your network then they can be scanned and ideally would be in scope, if not connected to the network it won’t be possible to scan those.  We can present a proposal for both as well, but it needs to be clarified as could mean a big difference between proposals received.**

Q)Web App - URL, no of user roles, function and purpose, Dynamic pages. level of risk/sensitivity of data. (We can do a code review separate to a Pen. Test if of interest) (We can put together a programme with code review in the 2nd year as a way to journey toward enhanced security posture but in manageable steps **A) 1 URL , User roles: 4+, Functions: 50+, Pages: 100+**

Q)O365 - Number of External IP's **– A) External IP: Two**

Q) Network (Internal) - Number of Internal IP's, locations, FW's (no. of configs) **A)** **3x Subnets with 510 address – however due to the ongoing COVID-19 Pandemic, this number is massively reduced. The number of hosts is currently averaging circa 15.**

Q) As part of the mandatory pass/fail compliance section of the IT, bidders are asked to confirm acceptance of Social Work England’s T&C “as the basis of the contract”.

To what extent, if any, would Social Work England be prepared to negotiate these terms?

For example, if a bidder proposed amendments to particular clauses (whilst still retaining the basis of the agreement), would this be considered a “non-compliant” bid and therefore be disqualified?

**A)** **Our preference would always be to contract based on our terms and conditions presented; without any amendments. If suppliers do have any reservations around particular clauses, we would advise for them to present any proposed amendments as part of their tender submission (a box should be able to be inserted below the disclaimer to add text).**

**These proposed amendments will not be taken into account when evaluating any tender submission, however, they will be taken into consideration as part of the final contract award (please refer to 17.4 of the ITT).**

**Should we deem any proposed amendment to be unsuitable, we will advise the supplier of this, and if they are unwilling to accept Social Work England’s stipulated wording, we reserve the right to exclude their tender submission from consideration, and if they receive the highest total score following the evaluation stage, re-award the contract to next highest scoring bidder.**

Q)How many Appliances/Servers/devices/switches in the LAN infrastructure are to be tested? **A) Minimal devices due to lockdown ~ 20 (inc Printers, laptops, Teams meeting rooms devices) 6 switches, 1 firewall.**

Q)How many Wireless SSID’s are within scope to test? **A) 2**

Q)Will VPN access be provided should it be necessary to help mitigate COVID restrictions? **A) We are currently setting up a VPN, however this may or may not be in place ready for the testing. We don’t hold any services on-prem it is all cloud based. However we do have some VM’s that are accessible remotely that would get you on the network.**

Q)Web Application Penetration Testing: Within the document, you request a report for potential vulnerabilities with your CRM – Could you confirm the version of the CRM you are using? Is this in-house or an off-the-shelf solution? **A) Appian 20.1 its ‘off the shelf’ but heavily customised.** Q)Microsoft Azure AD: Could you confirm which services you are using within Azure? Example Azure Active Directory? **A) Pretty minimal, Azure AD, some Enterprise apps, app registrations, and 1 subscription for the purposes of Visual Studio**

Q)Network Infrastructure – LAN/WiFi: Could you provide an up-to-date network diagram and topology along with any supporting documentation that relates to the current network infrastructure? **A) Yes, attached with IP’s removed (PLEASE ASK SOCIAL WORK ENGLNAD IF YOU REQUIRE THIS DOCUEMENTATION)**

Q)What percentage of testing do you envisage being onsite during the contract? **A) In respect to the percentage of testing being onsite during the contract, due to the current situation with COVID-19, only the Network Infrastructure will need to take place onsite in the short term. However, over the course of the contract, this may change.**

Q)You say suppliers need to hold CHECK certification, does that mean you wish all tests to be conducted as per NCSC CHECK guidance?  If not, is a percentage of the testing NCSC CHECK?

Do suppliers need to hold GREEN LIGHT status with NCSC CHECK?  i.e. have both infrastructure and application certified CHECK Team Leads?

You mention testers require CREST certifications, do suppliers require CREST membership?

You mention testers require TIGER or Cyber certifications, do you mean the CyberScheme certifications?

It is not mandatory to be a Cyber Exchange Member to conduct CHECK tests, can this be a nice to have rather than mandatory please?

**A) *It is a mandatory requirement that any Potential Provider has obtained/hold the necessary accreditation (in as much that they must be certified to one of the accreditations, whilst also being part of one of the penetration testing certification schemes):***

* ***ISO 27001 certified (Information Security Management);***
* ***Cyber Essentials certified;***
* ***Cyber Exchange member;***
* ***CHECK certification scheme;***
* ***CREST certification scheme;***
* ***Tiger certification scheme; and/or***
* ***Cyber certification scheme.”***

**Our requirement is that the potential provider must hold at least one of the cyber related certifications; so either ISO 27001 certified or Cyber Essentials certified, and in an ideal world, they would hold both. Further to this, we then require as a minimum for potential provider to be accredited under at least one of the penetration testing certification schemes:**

* **CHECK scheme (**[**https://www.ncsc.gov.uk/information/become-a-check-provider**](https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.ncsc.gov.uk%2Finformation%2Fbecome-a-check-provider&data=04%7C01%7Ccommercial.team%40socialworkengland.org.uk%7C5a9da59299494ee0101b08d88647a029%7C687e5818d7b4485783d1ddad97154a74%7C0%7C0%7C637406989469435589%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=d3EnYlWjb8gewdT%2FGZ2h5eID7WOrjpJXm3LKvzQ%2FA5A%3D&reserved=0)**)**
* **CREST (**[**https://www.crest-approved.org/**](https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.crest-approved.org%2F&data=04%7C01%7Ccommercial.team%40socialworkengland.org.uk%7C5a9da59299494ee0101b08d88647a029%7C687e5818d7b4485783d1ddad97154a74%7C0%7C0%7C637406989469435589%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=mLRpTftZh7Bk0G2%2F40HAgjyWTvQpioY6RIIr8f8lwXc%3D&reserved=0)
* **Tiger scheme (**[**https://www.tigerscheme.org/**](https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.tigerscheme.org%2F&data=04%7C01%7Ccommercial.team%40socialworkengland.org.uk%7C5a9da59299494ee0101b08d88647a029%7C687e5818d7b4485783d1ddad97154a74%7C0%7C0%7C637406989469445581%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=c9TrRWL0DIq6cztDa4Hy4oFVK49T0ZH41XjSzNkdXpk%3D&reserved=0)**)**
* **Cyber scheme (**[**https://www.thecyberscheme.org/**](https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.thecyberscheme.org%2F&data=04%7C01%7Ccommercial.team%40socialworkengland.org.uk%7C5a9da59299494ee0101b08d88647a029%7C687e5818d7b4485783d1ddad97154a74%7C0%7C0%7C637406989469455573%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=LsdNBAWmz369bZbzAH9QEZrAYGwXD4hE3ksFmbQDFd8%3D&reserved=0)**)**

Q) Can you confirm if you require NCSC CHECK ITHCs as opposed to a non-CHECK pentest? **A) If NCSC CHECK ITHC is possible, then yes.**

Q)How many Appliances/Servers/devices/switches in the LAN infrastructure are to be tested? **A)** **Minimal devices due to lockdown ~ 20 (inc Printers, laptops, Teams meeting rooms devices) 6 switches, 1 firewall**

Q)How many Wireless SSID’s are within scope to test? **A) 2**

Q) Will VPN access be provided should it be necessary to help mitigate COVID restrictions? **A) We are currently setting up a VPN, however this may or may not be in place ready for the testing. We don’t hold any services on-prem it is all cloud based. However we do have some VM’s that are accessible remotely that would get you on the network.**

Q) Regarding the additional elements, 10 days consultancy and 5 days contingency, are these per year or to be spread over the 2-3 years? **A) We envisioned the requirement to be per year.**

Q)The main question is regarding the 10 days consultation + 5 days contingency within the pricing element. Would you be able to confirm if this is 15 days per annum or 15 days over the three-year pricing? **A) Per year**

Q) In terms of the infrastructure element will this need to be conducted on-site? **A) In respect to the percentage of testing being onsite during the contract, due to the current situation with COVID-19, only the Network Infrastructure will need to take place onsite in the short term. However, over the course of the contract, this may change.**

Q) If onsite, do you have a set-policies regarding COVID restrictions and mitigations in place within the office? **A) We are COVID safe**

Q) Could you please confirm if you wish to see evidence of i.e. in an appendix, of: CREST, TIGER and/or Cyber Scheme qualifications/certifications, Mandatory accreditations i.e. ISO27001. **A) A bidder will need to have one at least one of the mandatory accreditation (e.g. ISO27001/Cyber Essentials), and be a part of at least one of the Pen testing schemes. A bidder will also need to stipulate within their bid submission which accreditations they hold/schemes they are part of, and provide the evidence of this (e.g. an appendix with a copy of the certification).**

Q) Are the wireless access points setup using the same configurations? If so, would testing a sample of wireless access points be suitable? **A) Yes all the AP’s have the same configuration**.

Q) Section 15.9 states:

* 1. Potential Providers are required to respond to all the price question below. Costs should be submitted via the cost matrix template provided. Please adjust as necessary the size of the ‘cost matrix’ template and/or the ‘response’ box in order to accommodate your response.

Can you please confirm if the matrix to be used is the one in the embedded document? Or is there another table to use please?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task** | **Net Cost** | **VAT**  | **Gross Cost** | **Invoice date** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| **Total** | **£** | **£** | **£** |  |

1. **No, that is the cost template from within the contract. Bidders should make their tender submission, providing pricing within the relevant section highlighted within Part B (page 27) please. Please discount point 15.9 – the wording of this section should have been amended accordingly.**

Q)Please can you clarify that the estimated budget costs of £35,000 is per year or is this the total budget for 3 years? **A)** **The Budget is £35,000 per financial year.**

Q) For clarity regarding the 10 day consultation and 5 day contingency will this need to come within the £35k Per year budget, or separate? **A) All days (estimated number of days for all Pen Testing, contingency days and consultation days) will need to come from the budget allocated per annum. Bidders should refer to 15.10 – “Potential Providers should note that the maximum budget for the provision of the required services is £35,000 (net) for each financial year – please note that this includes any days for consultation, remediation/ad hoc work and inbuilt contingency should it so be required. However, we would encourage Potential Providers to submit tenders at their ‘best possible price’ rather than aligning any submission with the maximum budget available (as the budget may be subject to change).”It should also be noted that we are seeking potential providers to offer day rates that represent the best value for money, and we would encourage tenders to be submitted at the ‘best possible price’ rather than aligning costs with the maximum budget that is available.**

**Web Application**

Q)Could you confirm the core functionality of these applications? **A)** **Our public facing CMS where our clients (Social Workers) register and upload CPD.**

Q)We have seen the URL socialworkengland.co.uk), which states that you do not use a COTS as CMS. By hoovering over some of the links on the website, it is possible to see references to "umbraco", which is a popular CMS tool. Could you please provide more technical information about the web site? i.e. programming language used, frameworks (i.e. MVC), backend/frontend/data-layer technologies, etc. **A) We use Appian CMS as the back end of the system, we use Umbraco as the website/front end.**

Q)We would also need 2 user accounts per user level. Would you be in the position to provide such accounts? **A) Yes**

Q)Based on the answers provided, we have identified your interest in internal infrastructure assessment of a LAN and a WLAN. Are you also interested in build/configuration review of network devices and/or external infrastructure assessments? **A) No**

**O365/Azure**

Q)Which is your type of licence and what are the services you are using from O365? **A)** **M365 E5. Used for Office, Exchange, SharePoint, OneDrive, Teams etc. Second tenant is M365 F3.** Q) Do you have concerns over a particular aspect of your environment/s? If so, please specify **A) We are aware there are lots of security elements and mechanism built into O365, we want to ensure we have a good set of rules in place, and are not missing something major.**

Q) Will other users be interacting with the environment/s at the time of the assessment? **A) Depending on the time, possibly.**

Q)Will developers or administrators be making any changes to the environments in scope at the time of the assessment? Note: NCC Group strongly recommend that no modifications be made to the target cloud environment/s during the assessment unless strictly necessary. **A) We can make sure they are not.**

Q) How many Azure subscriptions are in scope – please list each environment with its own set of resources. **A)** **Azure usage is currently at a minimum only one Sub with Visual Studio attached. This will increase over the lifetime of the contract. Currently mainly used for enterprise apps, SSO, identity management etc**

Q)How many regions are in scope e.g. UK South, UK West or others? **A)** **Our tenant is ‘United Kingdom’** Q)How many applications are hosted within each cloud environment? **A) None**

Q) If more than one, which environments are deemed of greatest importance and/or process the most sensitive data? **A) n/a**

**Q)** Which cloud services or components are being utilized by the environment(s) in scope? (E.g. VM instances, databases, ELB’s, object storage, event triggered app code, Lambda functions, etc.) **A) n/a**

Q) How many VPC’s, VNet’s or subnets are in use? **A) None**

Q)How many security groups are there? **A) 316**

Q)Approximate number of rules per security group? **A) None**

Q) Approximate number of network ACL rules/conditional access policies? e.g. EC2/VMs, RDS/Databases) **A) 12 CA policies**

Q)What type of databases are in use? E.g. SQL/RDS?DynamoDB/Cosmos **A) None**

Q)Number of IAM users and groups? **A) 419, 316**

Q) Number of IAM policies and roles in use? **A) 2**

Q) Number of storage objects in scope e.g. S3/Blob storage/Cloud storage **A) None**

Q) Are any cloud network diagrams available at this stage? **A) No**

Q)Has any form of hardening been applied to the existing cloud configuration? If so, can details be provided **A) No**

Q)Please provide the number of lines of code If using bespoke event triggered application services such as Lambda or Azure functions? **A) n/a**

Q)Are you utilizing any cloud containerization solutions? e.g. Kubernetes or Docker **A) No**

**LAN/Wireless Assessment**

Q)What are the specific goals of the wireless assessment? For example, do you have network design concerns or a suspected intrusion? **A) Ensure unauthorised access is blocked.**

Q)What is the role of the wireless networks, for example corporate email access or to facilitate Internet access for visitors? **A) 2 SSID, one for guests and personal devices, one for corporate devices.**

Q)Are any wireless protocols in use other than standard 802.11 networks (for example Bluetooth, Zigbee, LoRaWAN etc) **A) No**

Q)Has any work in relation to security already been performed on this wireless network? **A) Possibly**

Q) Is there a documented wireless security policy? **A) No**

Q)What are the make and models of the wireless equipment? **A) Cisco Meraki MX84, MR42 x14, MS225-24P**

Q)How many physical geographic locations require Wireless testing, and what is/are the address(es) of the locations? **A) 1, Sheffield**

Q)For the WLAN assessment, is you desire to get the access points assessed? If so, this might require onsite work to be performed, which will require extra due diligence process from our side in line with COVID procedures **A) No**

Q)Are access points centrally managed by a WLAN controller? **A) Yes**

Q)How do users authenticate to the wireless network (e.g. certificate, pre-shared key, domain credentials) **A) PSK**

Q)What types of authentication/encryption protocols are in place? (PEAP, EAP—TLS, WEP, WPA-PSK etc.) **A) WPA-PSK**

Q)Do you allow users to access the network from non-corporate devices? **A)** **Only on the guest SSID which is not connected to the corporate LAN**

Q)Are tunneling or VPN technologies used within the environment? **A) Currently being implemented although not live at the time of writing this**

Q)Are wireless intrusion detection systems in use? **A) No**

Q) Do you require a sweep for rogue access points? **A) Yes**