DCPP Supplier Assurance Questionnaire (SAQ)

Completing a Supplier Assurance Questionnaire

The Supplier Assurance Questionnaire (SAQ) is part of the Cyber Security Model. As a supplier, you must complete one each time you bid for a Ministry of Defence (MOD) contract.
You will:
- give some information about yourself and your organisation
- answer questions about the measures you have in place to protect against cyber threats
- find out whether you are compliant with the contract's Cyber Risk Profile

You must answer the questions relating to the contract's Cyber Risk Profile. For example, if the contract's Cyber Risk Profile is Moderate, you need to answer questions for the Very Low, Low and Moderate Cyber Risk Profiles.

Contract and context details

All suppliers must answer the questions in this section.

1

Your name

Diane Mee

2

Your email address

contracts@virtual-college.co.uk

3

Your organisation’s Dun & Bradstreet D-U-N-S number

123456789

23-995-8858

4

Provide a brief description of your organisation. Choose one option only.

- (●) **My organisation is an SME (small or medium-sized enterprise)**
- ( ) **I am a sole trader**
- ( ) **My organisation works from multiple locations**
- ( ) **My organisation has locations outside of the UK**

5

Risk Assessment Reference

848650908.

6

Contract name

701577505 - Future Defence Infrastructure Services (FDIS) Accommodation Estate Tier 2 Training

7

Contract description

ANALYSIS, DESIGN AND DELIVERY OF TRAINING PACKAGES TO SUPPORT THE MOBILISATION AND BUSINESS AS USUAL DELIVERY OF FDIS REGIONAL DELIVERY (RD) ACCOMODATION

8

Answer the following question to check which parts of the form you need to complete.

In support of this contract only, please indicate whether MOD Identifiable Information is, or will be, processed on MOD accredited ICT systems? Choose one option only.

- (●) **The ICT system(s) used have no accreditation**
- ( ) **The ICT system(s) used have MOD accreditation to process OFFICIAL or OFFICIAL-SENSITIVE information**
- ( ) **The ICT system(s) used are accredited to process SECRET or TOP SECRET information**

9

As your ICT systems have no accreditation, you must answer all the questions relevant to the contract's Cyber Risk Profile.

Check which questions you need to answer in the table below. Select the contract's Cyber Risk Profile and click 'Next' to view the first set of questions.

Once you have completed the questions for your Cyber Risk Profile, you must complete the Compliance section at the end of the form and then agree to the declaration before submitting your SAQ.

Questions required to be answered with No ICT Accreditation				
	Question Set Very Low	Question Set Low	Question Set Moderate	Q H
CRP Very Low	✓	X	X	X
CRP Low	✓	✓	X	X
CRP Moderate	✓	✓	✓	X
CRP High	✓	✓	✓	✓

- I am completing SAQ questions for a "Very Low" Cyber Risk Profile
- I am completing SAQ questions for a "Low" Cyber Risk Profile
- I am completing SAQ questions for a "Moderate" Cyber Risk Profile
- I am completing SAQ questions for a "High" Cyber Risk Profile

Very Low Cyber Risk Profile

You must answer the questions in this section if the contract's Cyber Risk Profile is Very Low, Low, Moderate or High.

10

VL01 Does your organisation have Cyber Essentials certification that covers the scope required for all aspects of the contract, and do you commit to maintaining this standard for the duration of the contract? Choose one option only.

- No
- No, but we have a plan to put this in place by the point of contract award
- *Yes

11

Certification body

ECSC

12

Certification number

IASME-CE-010268

Low Cyber Risk Profile

You must answer the questions in this section if the contract's Cyber Risk Profile is Low, Moderate or High.

13

L01 Does your organisation have an approved information security policy in place?

- ○ No
- ○ Yes, this is locally documented
- ◉ *Yes, we have a documented and maintained policy that considers as a minimum the following areas: information risk management regime, network security, user education and awareness, malware prevention, removable media controls, secure configuration, managing user privileges, incident management, monitoring, and home and mobile working (and physical security)
- ○ *Yes, we have a documented and maintained policy that considers as a minimum the following areas: information risk management regime, network security, user education and awareness, malware prevention, removable media controls, secure configuration, managing user privileges, incident management, monitoring, and home and mobile working (and physical security). This is based on a formal recognised standard and is independently verified

14

L02 Are information security relevant roles identified and responsibilities assigned within your organisation?

- No
- Yes, roles and responsibilities have been assigned, but are not documented
- *Yes, roles and responsibilities have been assigned, and are formalised in accordance with and form part of corporate policy
- *Yes, roles and responsibilities have been assigned, and are formalised in accordance with and form part of corporate policy and are effectively communicated throughout your organisation

15

L03 Does your organisation define and implement a policy that addresses information security risks within supplier relationships?

- No
- Yes, using company standards
- *Yes, and it ensures that all relevant 'cyber standards' required through contracts or regulation are flowed down
- *Yes, and it ensures that all relevant 'cyber standards' required through contracts or regulation are flowed down. We also have additional requirements that are flowed down as required

16

L04 Does your organisation define and implement a policy that ensures that all functions have sufficient and appropriately qualified resources to manage the establishment, implementation and maintenance of information security?

- No

*Yes

17

L05 Are employee and contractor responsibilities for information security formally defined?

- No
- Yes, guidance is given, but no acknowledgement is required
- *Yes, in the general terms and conditions of employment and/or corporate policy. (For the avoidance of doubt this should cover full-time employees, contractors and agency staff)

18

L06 Does your organisation ensure that personnel with information security responsibilities are provided with suitable training?

- No
- Yes, we provide general training but nothing specific to a role
- *Yes, we provide training as required to roles
- *Yes, we define minimum skill sets for specific roles and have a continuous education process in place to ensure our employees meet or exceed these

19

L07 Does your organisation have a policy for ensuring that sensitive information is clearly identified?

- No
- Yes, we identify such information but do not apply a formal classification to it
- *Yes, we identify such information and apply a formal classification scheme in accordance with our policies or regulatory requirements

- [ ] *Yes, we identify such information and apply a formal classification scheme in accordance with our policies or regulatory requirements, and communicate this to all staff to ensure they clearly understand the scheme and their responsibilities for ensuring it affords appropriate protection to sensitive information

20

L08 Does your organisation have a policy to control access to information and information processing facilities?

- [ ] No, we rely on our staff to do the right thing
- [ ] Yes, we have formal handling - storage, transmission, transportation, retention and disposal - procedures based on our classification scheme
- [x] *Yes, we have formal handling - storage, transmission, transportation, retention and disposal - procedures based on our classification scheme, and a policy that is documented and maintained
- [ ] *Yes, we have formal handling - storage, transmission, transportation, retention and disposal - procedures based on our classification scheme, which include handling in accordance with all regulatory requirements considered and captured in our baseline process

21

L09 Does your organisation have Cyber Essentials Plus certification that covers the scope required for all aspects of the contract, and do you commit to maintaining this standard for the duration of the contract?

- [ ] No
- [ ] No, certification is planned to be in place at the point of contract award
- [x] *Yes

22

Certification body

ECSC

23

Certification number

IASME-CE-001991

24

L09a If you do not have Cyber Essentials Plus certification, do you have an equivalent standard that you would like to claim as an alternative?

- No
- Yes

25

L10 Does your organisation have a policy to control the exchange of information via removable media?

- No, we rely on our staff to do the right thing
- Yes, we have handling procedures that are applied on a case-by-case basis
- *Yes, we assess the risks of the use of removable media and are managing it with a policy that is documented and maintained
- *Yes, we have a removable media policy which ensures that data held on removable media is the minimum necessary to meet the business requirement and is appropriately encrypted

26

L11 Does your organisation maintain the scope and configuration of the information technology estate?

- No, we have not established the scope and configuration of our IT estate
- Yes, we understand the size and topology of our corporate networks. We have a register of some, but not all assets
- *Yes, we have a verified understanding of the size and topology of our corporate networks. We have a register of all assets that is regularly reviewed
- *Yes, we have a verified, automated description of the size and topology of our corporate networks. We have an integrated, network-enabled register of all assets, which notifies us if an unknown asset is detected

27

L12 Does your organisation have a policy to manage the access rights of user accounts?

- No, we do not control access to information assets or maintain access records
- Yes, but we rely on procedural measures to control access to information assets
- *Yes, we have an access control policy which covers how we establish appropriate user access rights to ensure that users only have access to information necessary for them to perform their role. Access rights are granted on a 'least privilege' basis
- *We require multi-factor authentication for accounts that have access to sensitive data or systems; we employ technology to enforce access control lists (ACLs) even when data is recovered off a server; we maintain records of access to our information assets

28

L13 Does your organisation have a policy and deploy technical measures to maintain the confidentiality of passwords?

- No, we do nothing technical to maintain the confidentiality of passwords

- Yes, we have a policy
- *Yes, we have a policy and technically ensure that all passwords are cryptographically protected when transmitted or stored electronically
- *Yes, and in addition we ensure that password files can only be accessed by administrators with the business need and permissions to do so

29

L14 Does your organisation have a policy for verifying an individual's credentials prior to employment?

- No
- *Yes

30

L15 Does your organisation have a policy for all employees and contractors to report violations of information security policies and procedures without fear of recrimination?

- No
- *Yes

31

L16 Does your organisation have a disciplinary process in place to ensure that action is taken against those who violate security policy or procedures?

- No
- Yes, but this is just an informal process
- *Yes, we have a formal process, which is regularly reviewed and communicated to employees

32

L17 Does your organisation have procedures for information security incident management that include detection, resolution and recovery?

- No
- *Yes, we have a policy that is documented and maintained and includes what happens when there is suspicion or identification of a security incident, how this is reported through the organisation, and how the risk is isolated until resolved

33

L17a Which of the following information security incident management procedures apply to your organisation?

	Mark all that apply
We have procedures and responsibilities for incident response planning and management	
We have procedures for monitoring, detecting, analysing and reporting of information security events and incidents	
We have procedures for logging incident management activities	
We have procedures for handling (storage, transmission, transportation, retention and disposal) of forensic evidence	
We have procedures for response including those for escalation, controlled recovery from an incident and communication to	

internal and external people or organisations

34

L17b Does your organisation learn from information security incidents?

Mark all that apply

Yes, we have procedures for assessment of and decision on information events and assessment of information security weaknesses

Yes, we conduct regular reviews of effectiveness undertaken using the results of audits, incidents, measurements and feedback from interested parties

Moderate Cyber Risk Profile

You must answer the questions in this section if the contract's Cyber Risk Profile is Moderate or High.

35

M01 Does your organisation have a policy to ensure regular, formal information security related reporting? Choose one option only.

- No
- Yes, but only on an ad hoc basis (no regular formal reporting)
- *Yes, regular formal reporting arrangements are in place at board level or an equivalent senior responsible role

36

M02 Does your organisation have a policy that details specific employee and contractor responsibilities? Choose one option only.

- No
- Yes, we have a policy and make everybody aware before granting access
- *Yes, we have a policy and require confirmation before granting access

37

M03 Does your organisation use an appropriate and repeatable information security risk assessment process? Choose one option only.

- No
- *Yes, these are formalised in accordance with and form part of corporate policy
- *Yes, these are formalised in accordance with and form part of corporate policy, and the criteria for performing information security risk assessments and acceptable levels of risk are also defined and documented

38

M04 Does your organisation have a policy for storing, accessing and handling sensitive information securely? Choose one option only.

- No, we do not implement any measures to ensure privacy and protection of sensitive information
- *Yes, for information that is categorised as requiring enhanced protection (including legal, ITAR regulatory, contractual, sensitive personal) and we ensure it is protected in line with requirements
- *Yes, we have a policy and have designated roles within the organisation that provide guidance to managers, users and service providers on the individual responsibilities and the specific procedures that should be followed

39

M04a Do you ensure that any offshoring arrangements are in line with and meet HM Government and Ministry of Defence policy for the handling of such information? Choose one option only.

- No
- *Yes

40

M04b Do you ensure that any requests for bulk data transfers of such data are subject to formal approval before release (and are effected using secure and approved communications channels)? Choose one option only.

- No
- *Yes

41

M05 Does your organisation have a policy for data loss prevention? Choose one option only.

- No, we do not have a policy for data loss prevention
- No, we do not have a documented policy and rely on staff to do the right thing on a case-by-case basis
- *Yes, we have policy that defines what information may be released, and implement controls and monitoring to control the flow of data within the network and detect the unauthorised release of sensitive information
- *Yes, we have policy that defines what information may be released, and implement controls and monitoring to control the flow of data within the network (spotting and addressing any anomalies where traffic exceeds the normal) and detect the unauthorised release of sensitive information, and have back-up mechanisms in place

42

M06 Does your organisation have a policy for implementing and testing backups that are stored offline? Choose one option only.

- No, we do not implement any measures for backup and restoration
- No, we have online backups only
- Yes, we have offline backups and they are not tested regularly
- *Yes, we have scheduled offline backups that are stored securely and are tested regularly
- *Yes, I have arrangements with Service Provider(s) for backup and restoration services and it is tested regularly

43

M07 Does your organisation ensure that asset owners are identified and that they control access to these assets? Choose one option only.

- No
- *Yes, we have an inventory of our organisation's assets and ensure that all information-related assets have a defined owner who ensures that, where appropriate, assets have rules for their acceptable use

44

M08 Does your organisation manage vulnerabilities for which there are no countermeasures? Choose one option only.

- No, we do not do anything specific to address evolving vulnerabilities
- Yes, we recognise that there will be evolving vulnerabilities in our systems and take note of any advice we are made aware of
- *Yes, we subscribe to a vulnerability alerting service, formally review alerts and mitigate as a matter of priority

- *Yes, and in addition we manage risks to legacy systems, where possible isolating these systems, and/or providing additional protective controls and monitoring until they can be updated/replaced

45

M09 Does your organisation ensure that administrative access is performed over secure protocols using multi-factor authentication (MFA)? Choose one option only.

- No
- *Yes, admin access is performed via secure protocols (such as SSH) using 2FA as a minimum
- *Yes, administrative access is performed over a separate management network using secure protocols and MFA

46

M10 Does your organisation monitor network behaviour and analyse events for potential incidents? Choose one option only.

- No, we neither monitor our network nor analyse events for incidents
- Yes, we undertake ad hoc inspections of event logs but do not have a regular commitment to log analysis
- *Yes, we deploy network traffic monitoring tools and analyse and record the events they generate

47

M11 Has your organisation defined and implemented a policy for monitoring account usage and managing changes to access rights? Choose one option only.

- No
- Yes, but only through acceptable use policies and procedures

- *Yes, we actively control user access to user accounts through a corporatewide, technically enforced mechanism such as the use of a mandatory password complexity algorithm with managers actively matching staff with existing accounts. We monitor compliance to acceptable use policies and procedures through technical controls
- *Yes, (as above) but also implement additional measures (such as limiting and controlling access to the audit system, monitoring attempts to access deactivated accounts, or other measures)

48

M12 Does your organisation control remote access to its networks and systems? Choose one option only.

- No, we do nothing specific
- Yes, we ensure that permission is sought before granting access to external organisations or remote users
- *Yes, we control access to our networks and systems by ensuring that those approved to connect do so using approved mechanisms
- *Yes, as above and devices, and we actively confirm right to access, verify end point security and identify before connection is completed

49

M13 Does your organisation have a policy to control the use of authorised software? Choose one option only.

- No
- *Yes

50

M14 Does your organisation have a policy to control the flow of information through network borders? Choose one option only.

- No, we do nothing to control the flow of information through network borders

- Yes, we deny outgoing communications to known malicious IP addresses
- *Yes, we have a policy that controls access through either a 'Whitelist' or 'Blacklist' and control the use of authorised protocols
- *Yes, we employ intrusion protection devices, block known suspicious network behaviour and direct all outgoing traffic through an authenticated proxy server

51

M15 Does your organisation define and implement a policy for applying security vetting checks to employees? Choose one option only.

- No
- *Yes

52

M15a Which of the following vetting standards do you apply?

	Mark all that apply
National Security Vetting	
Baseline Personnel Security Standard (BPSS)	
Counter Terrorist Check (CTC)	
Security Check (SC)	
Developed Vetting (DV)	
Disclosure Scotland	
Standard Disclosure	
Enhanced Disclosure	
Protecting Vulnerable Groups scheme	

Other - provide details below

53

If you chose 'other', what other vetting standards do you apply?

Enter your answer

54

M16 Does your organisation undertake personnel risk assessments for all employees and contractors ensuring those with specific responsibilities for information security have sufficient qualifications and experience? Choose one option only.

- No
- Yes, we have a policy to undertake personnel risk assessments for all employees and contractors
- *Yes, we have a policy and we ensure those with specific responsibilities for information security have sufficient qualifications and experience

55

M17 Does your organisation have a policy to secure organisational assets when individuals cease to be employed? Choose one option only.

- No
- *Yes

High Cyber Risk Profile

You must answer the questions in this section if the contract's Cyber Risk Profile is High.

56

H01 Does your organisation maintain patching metrics and assess patching performance? Choose one option only.

- No, we do nothing specific
- Yes, we implement the controls stipulated in Cyber Essentials, but nothing extra
- *Yes, we have a policy that sets targets and processes that measure actual time to patch against policy requirements
- *Yes, as above, and the Board seeks formal reporting on these to approve, tune and action any resulting issues noted

57

H02 Does your organisation ensure that wireless connections are authenticated? Choose one option only.

- No, we have wireless devices but do nothing specific to secure their use
- *Yes, we have a wireless policy which outlines the best practice for wireless technology and manages the risk appropriately with a minimum encryption requirement of WPA2 or equivalent
- *Yes, we authenticate wireless connections and use CPA or other HM Government approved encryption products
- *Not applicable - we do not use wireless devices

58

H03 Does your organisation deploy network monitoring techniques that complement traditional signature based detection? Choose one option only.

- No, we do nothing specific

- *Yes, we deploy automated network monitoring devices using behaviour-based anomaly detection to complement signature-based detection
- *Yes, (as above) plus we monitor outputs and proactively respond to any trends noted to tune defences and improve monitoring activities

59

H04 Does your organisation place application firewalls in front of critical servers to verify and validate the traffic going through the server? Choose one option only.

- No
- *Yes

60

H05 Does your organisation deploy network based IDS sensors on ingress and egress points within the network and update regularly with vendor signatures? Choose one option only.

- No, we do nothing specific
- *Yes, we have deployed network intrusion detection and monitor the logs
- *Yes, we have deployed network intrusion devices and monitor logs to spot trends, tuning monitoring and amending policies accordingly as part of a formal review process

61

H06 Does your organisation define and implement a policy to control installations of and changes to software on any systems on the network? Choose one option only.

- No, we do nothing specific
- Yes, we have a policy, but rely on staff to do the right thing

- *Yes, we have a policy, create a known secure configuration and utilise file and system integrity checking tools to verify that known secure configurations are maintained
- *Yes, (as above) plus we proactively look for and remove unauthorised software, ensuring permissions to install and change software are actively controlled. Acceptable behaviours are set out in policy and the disciplinary consequences of failure to follow these policies are explained to staff during induction and in follow on training activities

62

H07 Does your organisation control the flow of information through network boundaries and police the content by looking for attacks and evidence of compromised machines? Choose one option only.

- No
- *Yes

63

Explain your answer

Enter your answer

64

H08 Does your organisation ensure that networks are designed to incorporate security countermeasures, such as segmentation or zoning? Choose one option only.

- No
- Yes, we do separate our internal and external facing networks using firewalls to create DMZ
- *Yes, we identify critical assets (and business functions) and provide appropriate additional protection e.g. through segmentation, zoning, isolating or other additional controls

- *Yes, we have networks designed to provide differing levels of trust using recognised standards and approaches which are formally accredited

65

H09 Does your organisation ensure data loss prevention (DLP) at network egress points to inspect the contents of and, where necessary, block information being transmitted outside of the network boundary? Choose one option only.

- No, we do nothing specific
- *Yes, we inspect content for certain sensitive information (such as personal data, email classifications, and keywords)
- *Yes, and in addition we continually refine/tune our controls to improve our boundary defences

66

H10 Does your organisation proactively verify that the security controls are providing the intended level of security? Choose one option only.

- No, we do not review our processes or procedures
- Yes, we monitor and review processes and procedures on an ad-hoc basis as and when issues are identified
- *Yes, we conduct regular, independent reviews involving audits and testing

67

H11 Have you implemented a policy to ensure the continued availability of critical assets/information during any crisis? Choose one option only.

- We have local plans, but these are not formalised or documented
- *We have formal, documented plans that are subject to review
- *We have formal, documented plans that are reviewed and tested (and these form part of our wider organisational business continuity and disaster recovery plans)

Compliance

Are you compliant with the Cyber Risk Profile for the contract?

68

For each of the Cyber Risk Profile questions, asterisks show the compliant answers. Are all your answers compliant?

- All the answers I have given are compliant (marked with an asterisk)
- Some of the answers I have given are not compliant (not marked with an asterisk)

Declaration

All suppliers must read this information and confirm the statements to continue.

69

I have authority to complete the Supplier Assurance Questionnaire

The answers provided have been verified with all appropriate personnel and are believed to be true and accurate in all respects

All information which should reasonably have been shared has been included in the responses to the questions

Should any of the information on which the responses to this Supplier Assurance Questionnaire are based change, my company undertakes to notify the Ministry of Defence as soon as is reasonably practicable

My company acknowledges that the Ministry of Defence reserves the right to audit the responses provided at any time
*

- **For and on behalf of my company, I confirm the above statements.**

70

What happens next *

Click the 'Submit' button below to submit your Supplier Assurance Questionnaire (SAQ).

You will receive an email to the email address you gave to confirm whether you are compliant with the contract's Cyber Risk Profile. This email will also include your SAQ Reference.

- [ ] **I understand the information above**