Supplier Assurance Questionnaire (SAQ) for a contract with a Low Cyber Risk Profile

How to use this form

This Supplier Assurance Questionnaire (SAQ) is part of the Cyber Security Model.

You will need to:

- complete the SAQ to give information about yourself, your organisation and the measures you have in place to protect against cyber threats
- submit the completed SAQ to the Cyber & Supply Chain Security (CSCS) team (UKStratComDD-CyDR-DCPP@mod.gov.uk.)
- check the email you will receive back from the CSCS team – this will confirm whether you are compliant with the contract's Cyber Risk Profile, and should arrive within 2 working days
- keep copies of the completed SAQ and the email you receive from the CSCS team and attach them when you submit your tender response

Check whether you are compliant with the contract's Cyber Risk Profile before you submit the SAQ

For each of the Cyber Risk Profile questions, asterisks show the compliant answers. If you give an answer that is not compliant, you must answer an extra question before the declaration at the end of the form.

Where possible send a completed PDF via email, rather than a scan of a printed version (scanned submissions will take longer to process)

Section 1 Context and contract details

Risk Assessment Reference (RAR) for this contract

R	A	R	—	

(This should be populated when you receive this form. If not, please return to MOD)

Your name

Your email address

Your Organisation’s Name

Who is responsible for Information Security in support of this contract?

Full Name:
Email Address:
Contact Phone Number:

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

If you do not have one, you can request one for free on Dun & Bradstreet’s website at https://www.dnb.co.uk/duns-number/lookup/request-a-duns-number.html

Is this form being completed as an Annual SAQ Renewal or Is this the first SAQ to be completed for this contract?

□ First Completion for this contract

□ On major change to delivery of contract (Please add previous SAQ reference)

Which statement best describes your organisation? Tick all the boxes that apply.

□ 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

Bid / Contract Details

Bid / Contract name

Bid / Contract description

(Max 50 words, OFFICIAL information only)

Section 2 MOD Accreditation

In support of this contract only, please indicate whether MOD Identifiable Information is, or will be, processed on MOD accredited ICT systems. If the system you will use to support this contract is accredited, please enter the DART name and/or ID.
There is no waiver against DEF STAN 05-138.

□ The ICT systems we will use, have no MOD accreditation

□ The ICT systems we will use for OFFICIAL-SENSITIVE have MOD Accreditation (Please detail Below)

□ The ICT systems we will use have current MOD accreditation to process data at the appropriate classification (Please detail below)

Dart System 1 Name

TOA Reference

(Dart References can be TOA- or S-)

Dart System 2 Name

TOA Reference

(Dart References can be TOA- or S-)

Dart System 3 Name

TOA Reference

(Dart References can be TOA- or S-)

Section 3 Security Certification

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 (Please complete the Cyber Implementation Plan)

□ No, but we have a plan to put this in place by the point of contract award (Please complete the Cyber Implementation Plan)

□ *Yes (add the certification details below)

Certification body

Certification number

Certification expiry date (DDMMYY)

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? Choose one option only.

□No (Please complete the Cyber Implementation Plan)

□No, but certification is planned to be in place at the point of contract award (Please complete the Cyber Implementation Plan)

□*Yes (add the certification details below)

Certification body

Certification number

Certification expiry date (DDMMYY)

Please complete all the following questions even if you have declared certification above.

Section 4 Governance

L01 Does your organisation have an approved information security policy in place? Choose one option only.

❑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 all the areas listed in the previous answer. This is based on a formal recognised standard and is independently verified

L02 Are information security relevant roles identified and responsibilities assigned within your organisation? Choose one option only.

❑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

L03 Does your organisation define and implement a policy that addresses information security risks within supplier relationships? Choose one option only.

❑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

Section 5 Security Culture and Awareness

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? Choose one option only.

❑No

❑*Yes

L05 Are employee and contractor responsibilities for information security formally defined? Choose one option only.

❑No, there is nothing formal in place

❑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)

L06 Does your organisation ensure that personnel with information security responsibilities are provided with suitable training? Choose one option only.

❑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

Section 6 Information Asset Security

L07 Does your organisation have a policy for ensuring that sensitive information is clearly identified? Choose one option only.

❑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

L08 Does your organisation have a policy to control access to information and information processing facilities? Choose one option only.

❑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

❑*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

Section 7 Info-Cyber Systems Security

L10 Does your organisation have a policy to control the exchange of information via removable media? Choose one option only.

❑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

L11 Does your organisation maintain the scope and configuration of the information technology estate? Choose one option only.

❑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

L12 Does your organisation have a policy to manage the access rights of user accounts? Choose one option only.

❑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

L13 Does your organisation have a policy and deploy technical measures to maintain the confidentiality of passwords? Choose one option only.

❑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

Section 8 Personnel Security

L14 Does your organisation have a policy for verifying an individual's credentials prior to employment? Choose one option only.

❑No

❑*Yes

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? Choose one option only.

❑No

❑*Yes

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

❑No

❑Yes, but this is just an informal process

❑*Yes, we have a formal process, which is regularly reviewed and communicated to employees

Section 9 Security Incident Management

L17 Does your organisation have procedures for information security incident management that include detection, resolution and recovery? Choose one option only.

❑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

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

L17b Does your organisation learn from information security incidents? Tick all the boxes 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

If you are not compliant with the Cyber Risk Profile for the contract

For each of the Cyber Risk Profile questions, asterisks show the compliant answers. If you give an answer that is not compliant, you must answer the question below.

When will compliance be achieved? Choose <u>one</u> option only.

❑ Before contract commencement and we will provide a Cyber Implementation Plan (CIP) with this response

❑ Not before contract commencement, but we have provided a Cyber Implementation Plan (CIP) with this response

❑ We will be unable to achieve compliance we have provided a Cyber Implementation Plan (CIP) with this response

Guidance on Cyber Implementation Plans (CIPs) can be found at:
https://www.gov.uk/government/publications/cyber-implementation-plan-cip

Section 10 Declaration

All suppliers must read this information and tick the box to confirm agreement before submitting a Supplier Assurance Questionnaire.

- 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

Name:	(Type Name)
Email Address:	
Mobile Phone Number:	

Carefully check that you have responded to every relevant question before you submit your SAQ.

You will need to attach copies of your completed SAQ\CIP and the email you receive from the Cyber Supply Chain Security team when you submit your tender response.

Where possible send a completed PDF via email, rather than a scan of a printed version to UKStratComDD-CyDR-DCPP@mod.gov.uk