

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

How to use this form

The 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 DCPD team (ISSDes-DCPD@mod.gov.uk)
- check the email you receive from the DCPD 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 DCPD 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.

Context and contract details

All suppliers must answer these questions.

Your name

Your email address

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>

--	--	--	--	--	--	--	--	--

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

Risk Assessment Reference (RAR) for the contract

R	A	R	—									
---	---	---	---	--	--	--	--	--	--	--	--	--

Contract name

--

Contract description

--

Check which sections you need to complete

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 systems used have no accreditation

You must:

- answer all the questions in the form
- agree to the declaration at the end of the form

☐ The ICT systems have MOD accreditation to process OFFICIAL or OFFICIAL-SENSITIVE information

You do not need to answer the questions for the Very Low and Low Cyber Risk Profiles. You must:

- answer the questions for the Moderate Cyber Risk Profile
- agree to the declaration at the end of the form
- add the DART (Defence Assurance Risk Tool) name and/or ID below

☐ The ICT systems are accredited to process SECRET or TOP SECRET information

You do not need to answer the questions for any of the Cyber Risk Profiles. You must:

- agree to the declaration at the end of the form
- add the DART (Defence Assurance Risk Tool) name and/or ID below

If your ICT system(s) is accredited, enter the DART name and/or ID

Dart name

Dart ID

Very Low Cyber Risk Profile

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 (add the details below and go to question L01)

Certification body

Certification number

VL01a If you do not have Cyber Essentials certification, do you have an equivalent standard that you would like to claim as an alternative? Choose one option only.

- ☐ No (go to question L01)
- ☐ Yes

Low Cyber Risk Profile

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

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

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

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
- ☐ No, but certification is planned to be in place at the point of contract award
- ☐ *Yes (add details below and go to question L10)

Certification body

Certification number

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? Choose one option only.

- ☐ No
- ☐ Yes

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

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

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

Moderate Cyber Risk Profile

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

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

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

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

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

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

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

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, we have arrangements with Service Provider(s) for backup and restoration services and it is tested regularly

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

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

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

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

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)

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

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

- ☐ No
- ☐ *Yes

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

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

- ☐ No
- ☐ *Yes

M15a Which of the following vetting standards do you apply? Tick all the boxes 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 (add names below)

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

--

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

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

- ☐ No
- ☐ *Yes

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 one option only.

- ☐ Before contract commencement
- ☐ Not before contract commencement, but we will provide a Cyber Implementation Plan (CIP)
- ☐ We will be unable to achieve compliance

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

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 and the email you receive from the DCPD team when you submit your tender response.