



Defence Cyber  
Protection Partnership

Guidance

**Cyber Security Model:**

**Supplier Assurance Questionnaire (SAQ)  
Question Set Guide**

**December 2019**

# Contents

2. How to use this guide .....	2
3. Cyber Risk Profile Requirements.....	3
4. General Contract Context questions .....	4
5. Cyber Risk Profile: Very Low .....	5
6. Cyber Risk Profile: Low .....	5
7. Cyber Risk Profile: Moderate.....	9
8. Cyber Risk Profile: High .....	14
9. Sub-contracting.....	16

## 1. What is the Supplier Assurance Questionnaire (SAQ)?

The Supplier Assurance Questionnaire (SAQ) allows suppliers to demonstrate compliance with the cyber security controls required by a contract and its Cyber Risk Profile.

The SAQ forms part of the Defence Cyber Protection Partnership (DCPP) Cyber Security Model. The Authority<sup>1</sup> will first perform a Risk Assessment (RA) of the contract to determine its Cyber Risk Profile. Suppliers invited to tender then complete an SAQ to demonstrate their compliance.

Suppliers intending to sub-contract part of a Ministry of Defence contract will also be required to complete a Risk Assessment for any sub-contract(s), and sub-contractors will be required to complete an SAQ in response to it.

An SAQ is not required for contracts assessed as Not Applicable, however suppliers are still recommended to achieve Cyber Essentials certification.

For more information about the Cyber Security Model and the Defence Cyber Protection Partnership, visit: <https://www.gov.uk/guidance/defence-cyber-protection-partnership>

## 2. How to use this guide

This guide includes a workflow diagram of the questions which must be completed by suppliers when completing an SAQ. Both the Cyber Risk Profile of the relevant contract and the answers provided by a supplier will determine which questions are asked.

The question references (e.g. VL01) in the workflow refer to the full question and answer options listed on pages 4 to 9. Use both the workflow and the questions to understand what information will be required when responding to the SAQ.

**The response options highlighted in green and with an Asterix represent the minimum requirements to be compliant with the related controls for a contract with the specified Cyber Risk Profile.** Additional response options are also included, above the required compliance level, to evaluate cyber resilience across the Defence sector.






To view associated question-level guidance, visit Supplier Cyber Protection, the online service at <https://supplier-cyber-protection.service.gov.uk/> and complete a sample SAQ.

---

<sup>1</sup> The Authority is the person accountable for determining the Cyber Risk Profile appropriate to a contract and, where the contractor has not already been notified of the Cyber Risk Profile prior to the date of this contract, shall provide notification of the relevant Cyber Risk Profile and cyber security instructions as soon as reasonably practicable; and notify the contractor as soon as reasonably practicable where The Authority reassesses the Cyber Risk Profile relating to a specific contract.

### 3. Cyber Risk Profile Requirements

**Cyber Risk  
Profile:**

Not applicable		Recommended only	
Very Low			
Low		Plus additional controls for Low	
Moderate		Plus additional controls for Low	Plus additional controls for Moderate
High		Plus additional controls for Low	Plus additional controls for Moderate Plus additional controls for High

### 3. SAQ questions

**SAQ3 Do you have a Risk Assessment Reference?**

Yes - provide

No

**SAQ3a Which Cyber Risk Profile do you want to complete an SAQ against?**

Very Low

Low

Moderate

High

**SAQ4 Provide a name and description for the contract.**

### 4. General Contract Context questions

These questions will not determine whether you meet the minimum required standard for the contract's Cyber Risk Profile

**GCC02 Provide a brief description of your organisation, to help us understand your business context. Tick all that apply.**

My organisation is an Small Medium Enterprise (SME)

I am a sole trader

My organisation works from multiple locations

My organisation has locations outside of the UK

**GCC03 Do you have any of the following existing information security certifications or accreditations that provide evidence of your ability to operate securely at this level? Tick all that apply.**

<List of options, including "other" with text box for additional information>

**GCC04 In support of this contract only, please indicate whether MOD Identifiable Information is, or will be, processed on MOD accredited ICT systems?**

The ICT system(s) used has no accreditation

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

The ICT system(s) used is accredited to process SECRET or TOP SECRET information

## 5. Cyber Risk Profile: Very Low

**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?

No

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

\*Yes, provide certificate body and certificate no

**VL01a** Do you have an equivalent standard to Cyber Essentials certification that you would like to claim as an alternative?

No

Yes

**VL01b** Confirm which of the following statements apply to your organisation in the context of the equivalent standard you are claiming.

Boundary firewalls and internet gateways (list of statements)

Secure configuration (list of statements)

Access control (list of statements)

Malware protection (list of statements)

Patch management (list of statements)

## 6. Cyber Risk Profile: Low

**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: (list of information security policies areas)

Yes, we have a documented and maintained policy that considers as a minimum the following areas:

- (list of information security policy areas)
- 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?**
- 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?**
- 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?**
- No *\*Yes*
- L05 Are employee and contractor responsibilities for information security formally defined?**
- 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?**
- 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 that our employees meet or exceed these

- 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 any 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?**
- 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?**
- No
- No, certification is planned to be in place at the point of contract award
- \*Yes, provide certification body and certificate no*
- L09a Do you have an equivalent standard to Cyber Essentials Plus certification that you would like to claim as an alternative?**
- No Yes
- 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

- 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
- 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
- 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
- L14 Does your organisation have a policy for verifying an individual's credentials prior to employment?**  
 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?**  
 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?**  
 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?**  
 No \*Yes
- L17a Which of the following information security incident management procedures apply to your organisation? Tick 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
- L17b Does your organisation learn from information security incidents? Tick 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

## 7. Cyber Risk Profile: Moderate

- M01 Does your organisation have a policy to ensure regular, formal information security related reporting?**  
 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 for information security before granting access to sensitive assets?**
- 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?**
- 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?**
- 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?**
- 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)?**
- No *\*Yes*

- M05 Does your organisation have a policy for data loss prevention?**  
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?**  
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
- M07 Does your organisation ensure that asset owners are identified and that they control access to these assets?**  
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?**  
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)?**  
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?**  
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?**  
No  
Yes, but only through acceptable use policies and procedures  
\*Yes, we actively control user access to user accounts through a corporate-wide, 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?**  
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 policy to control the use of authorised software?**  
No \*Yes

- M14 Does your organisation have a policy to control the flow of information through network borders?**  
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?**  
No *\*Yes*
- M15a Which of the following vetting standards do you apply? Tick 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 name
- 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?**  
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?**  
No *\*Yes*

## 8. Cyber Risk Profile: High

- H01 Does your organisation maintain patching metrics and assess patching performance?**
- 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
- 
- H02 Does your organisation ensure that wireless connections are authenticated?**
- 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
- 
- H03 Does your organisation deploy network monitoring techniques that complement traditional signature based detection?**
- 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
- 
- H04 Does your organisation place application firewalls in front of critical servers to verify and validate the traffic going through the server?**
- No     \*Yes
- 
- H05 Does your organisation deploy network based IDS sensors on ingress and egress points within the network and update regularly with vendor signatures?**
- 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

- H06 Does your organisation define and implement a policy to control installations of and changes to software on any systems on the network?**
- 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
- 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?**
- No, explanation
- \*Yes, explanation*
- H08 Does your organisation ensure that networks are designed to incorporate security countermeasures, such as segmentation or zoning?**
- 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
- 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?**
- 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
- H10 Does your organisation proactively verify that the security controls are providing the intended level of security?**
- 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*

- H11 Have you implemented a policy to ensure the continued availability of critical assets/information during any crisis?**  
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)

## 9. Sub-contracting

- SC01 Will your organisation sub-contract any part of this contract?**  
No  
Yes  
Unknown

### Supplier Assurance Questionnaire Reference

You should complete a Risk Assessment for all of the elements you sub-contract.

Enter this SAQ Reference when asked for, to link that sub-contract and your bidding sub-contractors to this contract.

### SC03 Declaration

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.**