Scottish Cyber Assessment Service

Webinar for Public Sector Suppliers

Paul Chapman

Head of Public Sector Cyber Resilience

Scottish Government
Riaghaltas na h-Alba
gov.scot

Cyber Security Procurement Support Tool

Webinar for Public Sector Suppliers

Paul Chapman

Head of Public Sector Cyber Resilience

Scottish Government
Riaghaltas na h-Alba
gov.scot

The Cyber Threat

You may be wondering why you need to be concerned about cyber security and resilience.

Smaller public sector organisations often ask: “Why would anyone attack us?”

But if you or your suppliers rely on Internet-connected digital services or products to deliver public services, your organisation and the services you provide to the public are at risk.

Supplier Cyber Security

- Supply chain often a significant vulnerability for more mature organisations

- The Scottish public sector is being encouraged to ensure its suppliers have appropriate cyber security in place. That's because:

    - Duty to prevent disruption to vital public services
    - We want to support our suppliers to improve their cyber security

Supplier Cyber Security – What Are We Doing?

To help achieve this, the Scottish public sector have been encouraged to implement:

- A **guidance note** (embedded in the **Cyber Resilience Framework**) which has been produced for all public sector organisations, setting out best practice from the National Cyber Security Centre (the UK technical authority on cyber security).

- A beta decision-making support tool called the **Scottish Cyber Assessment Service**, which all public sector organisations and suppliers bidding for public sector contracts can make use of.

Supplier Cyber Security – Guidance Note

- **Key Point 1:** Follow the cyber security principles (the 12 Principles of Supply Chain Security) endorsed by the NCSC.
- **Key Point 2:** In particular, broadly align approach to NCSC Principle 5 ("Set and communicate minimum security requirements for suppliers") with the "Use Cases" provided by the NCSC.
- **Key Point 3:** Embed in procurement processes an appropriate and proportionate information/cyber security assurance process.
- **Key Point 4:** Proportionate, case-by-case approach to certification.

Scottish Cyber Assessment Service

Aims:

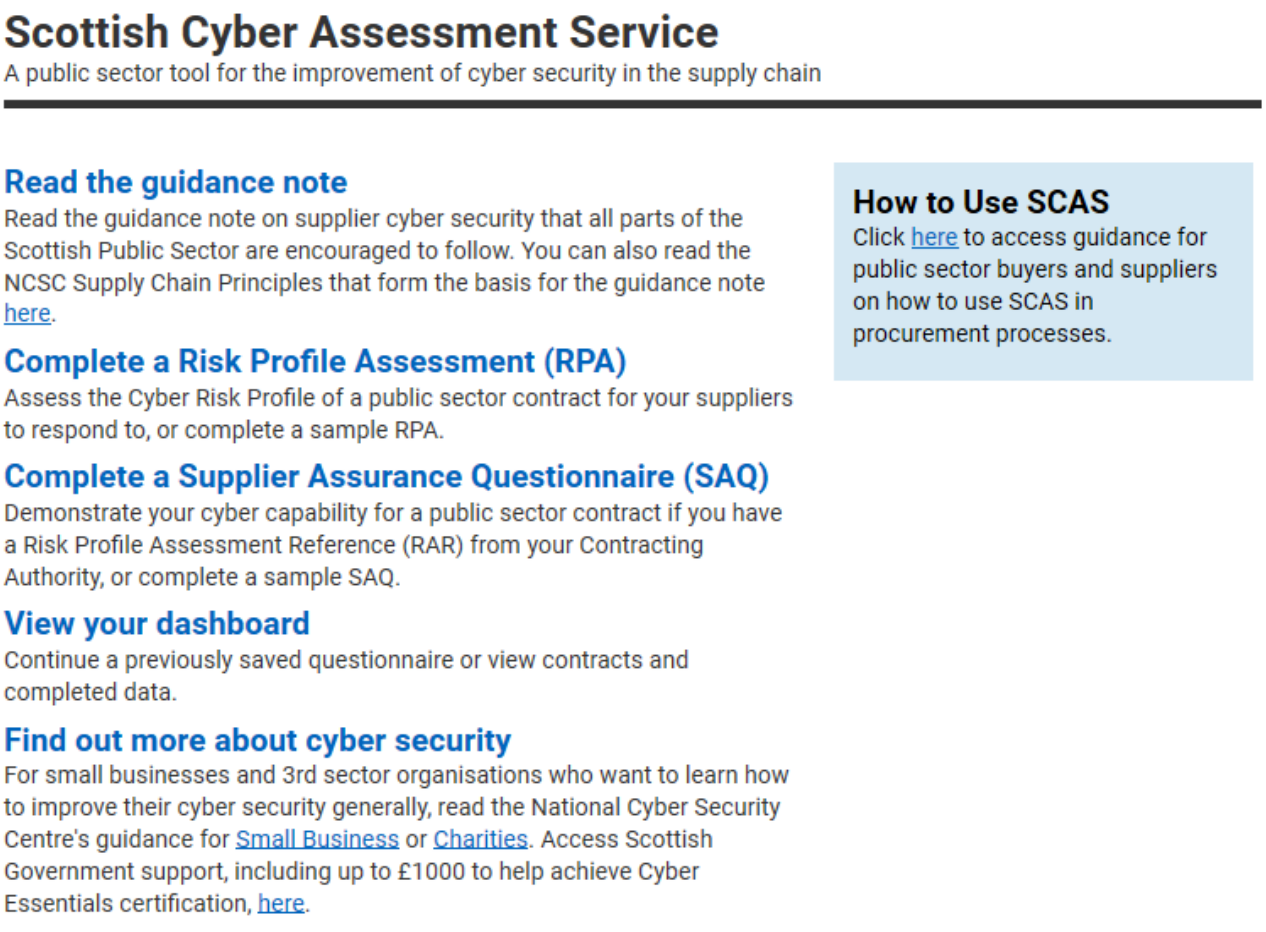
- Developed to support consistent implementation of a new Guidance Note, and produce richer information on supplier cyber security.

- minimise any necessary additional burdens on Scottish public sector organisations (as purchasers) and private and third sector organisations (as suppliers);

Scottish Cyber Assessment Service

	Scenario	Is SCAS suitable?
Class of contract or framework	"Standalone" contracts	✓
	Putting in place single supplier framework agreements	✓
	Contracts "called off" under multi- or single supplier framework agreements	✓
	Putting in place multi-supplier agreements/ dynamic purchasing systems[5]	✗
Type of criteria	Identifying and assessing against ESPD selection criteria	✗
	Identifying and assessing against minimum pass/fail contract award criteria	✓
	Identifying and assessing against more sophisticated scored cyber security contract award criteria[6]	✗

Scottish Cyber Assessment Service (SCAS) Tool



Scottish Cyber Assessment Service

A public sector tool for the improvement of cyber security in the supply chain

Read the guidance note

Read the guidance note on supplier cyber security that all parts of the Scottish Public Sector are encouraged to follow. You can also read the NCSC Supply Chain Principles that form the basis for the guidance note here.

Complete a Risk Profile Assessment (RPA)

Assess the Cyber Risk Profile of a public sector contract for your suppliers to respond to, or complete a sample RPA.

Complete a Supplier Assurance Questionnaire (SAQ)

Demonstrate your cyber capability for a public sector contract if you have a Risk Profile Assessment Reference (RAR) from your Contracting Authority, or complete a sample SAQ.

View your dashboard

Continue a previously saved questionnaire or view contracts and completed data.

Find out more about cyber security

For small businesses and 3rd sector organisations who want to learn how to improve their cyber security generally, read the National Cyber Security Centre's guidance for Small Business or Charities. Access Scottish Government support, including up to £1000 to help achieve Cyber Essentials certification, here.

How to Use SCAS

Click here to access guidance for public sector buyers and suppliers on how to use SCAS in procurement processes.

Scottish Cyber Assessment Service (SCAS) Tool

How does the Scottish Cyber Assessment Service work? (1)

- Public sector organisations are encouraged to use the tool to complete a **Cyber Risk Profile Assessment** for contracts before they issue Invitations to Tender.

- This will generate a **Cyber Risk Profile** for the contract, and a **Supplier Assurance Questionnaire** that is proportionate to the risk.

Scottish Cyber Assessment Service (SCAS) Tool

How does the Scottish Cyber Assessment Service work? (2)

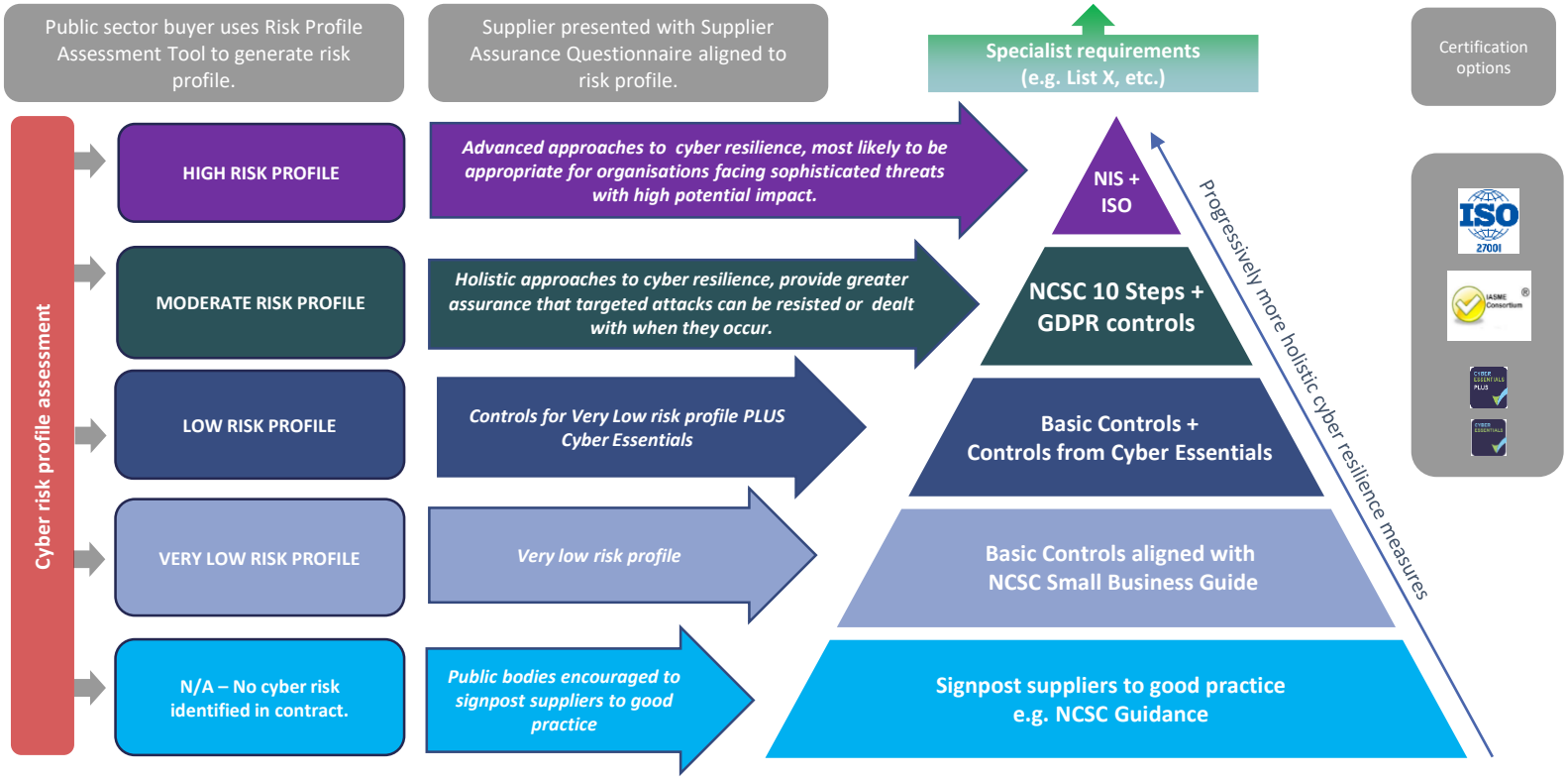
- A unique Risk Assessment Reference is generated by the service. This can be issued as part of the Invitation to Tender, along with the automatically generated information on cyber resilience requirements.

- Suppliers can use the Risk Assessment Reference to log onto the Tool, complete the relevant Supplier Assurance Questionnaire, and download a report to submit alongside all other tender documents.

- They will then be able to assess the answers provided by potential suppliers as part of their evaluation of tenders.

These are the **Common Core Cyber Resilience Requirements** that suppliers are expected to meet in order to manage cyber risk in Scottish public sector contracts. These requirements broadly align with NCSC Supply Chain Guidance, and are embodied in the SCAS decision-making support tool available at www.cyberassessment.gov.scot.

Public sector organisations may choose to **supplement these common core requirements** with additional controls or requirements depending on the circumstances of the contract and risk appetite. By ensuring they meet these common core requirements, suppliers can ensure they are well placed to manage cyber risk to an appropriate level when dealing with public sector contracts.



CiSP

Membership of the Cyber Security Information Sharing Partnership (CiSP) is encouraged to ensure threat intelligence awareness and sharing.

Incident reporting

Organisations should report significant cyber incidents to NCSC, Police Scotland, and appropriate authorities dependent on status (e.g. NIS Competent Authorities, ICO, etc.)

Triggers

Where organisations are using cloud services or cloud - enabled products, they will be asked to confirm compliance with **NCSC Cloud Security Principles.**

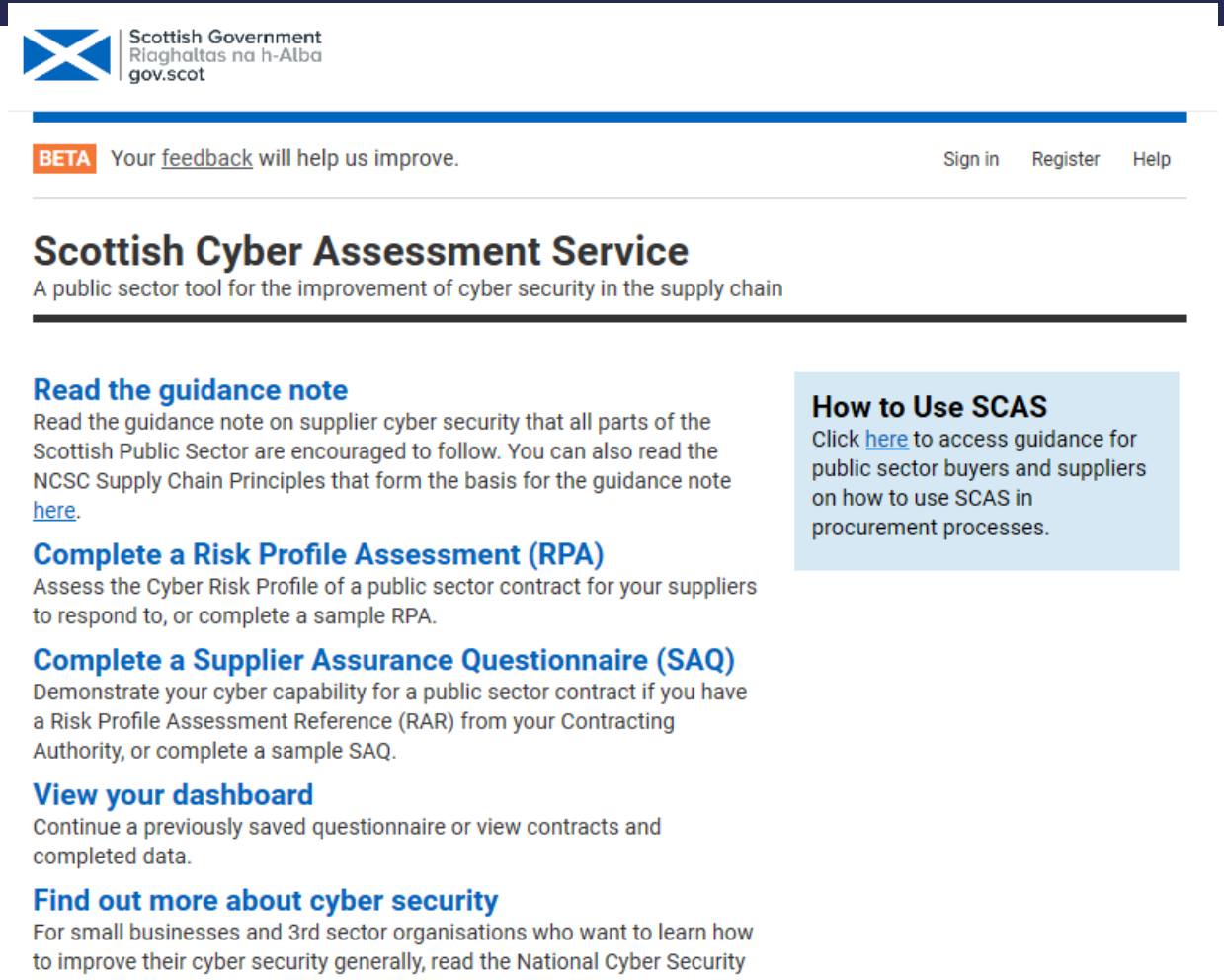
Triggers

Where personal information is processed, organisations will be asked to confirm compliance with **ICO/NCSC guidance for protecting personal data.**

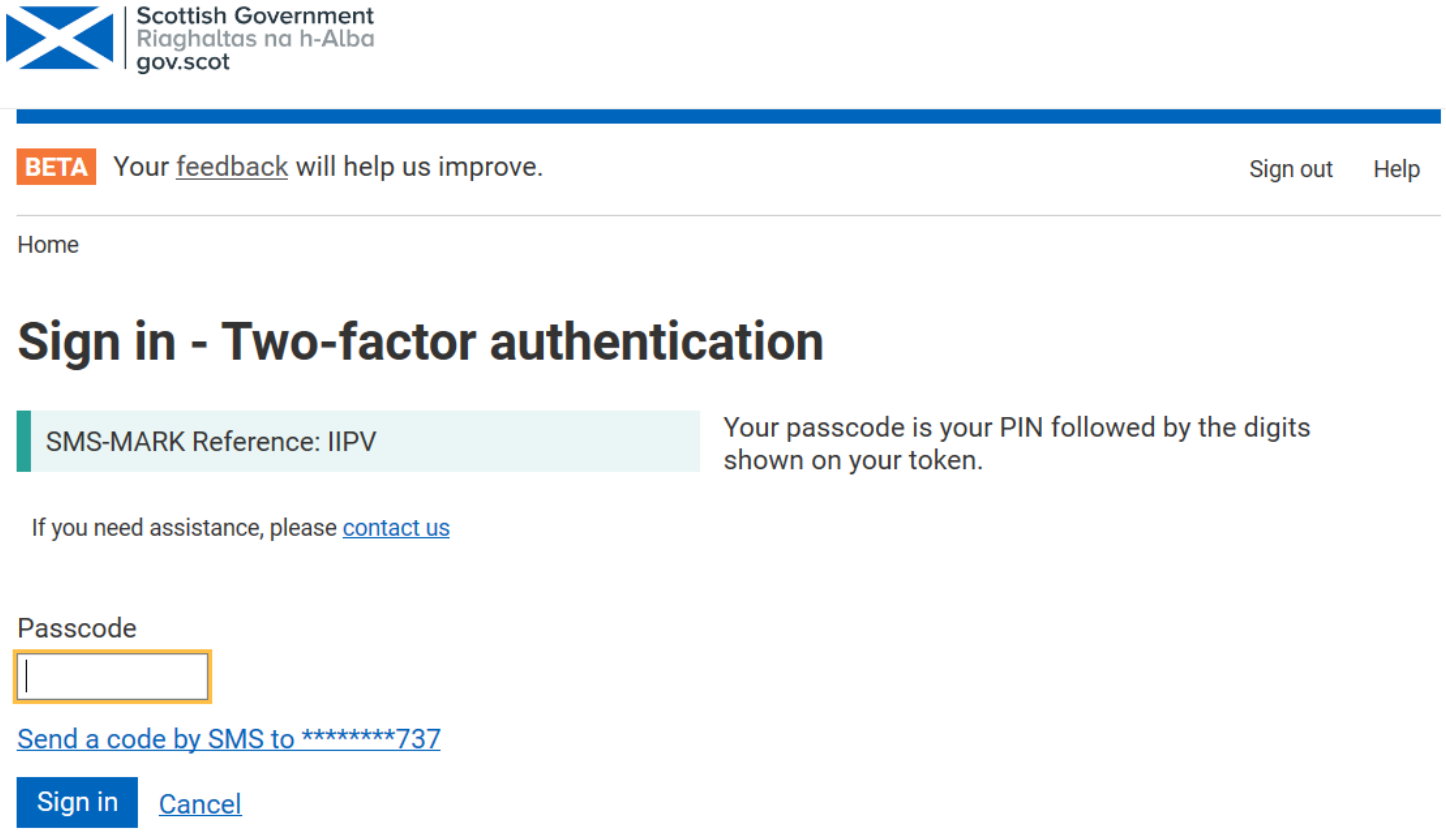
Triggers

Where payment card data is processed, organisations will be asked to confirm compliance with **PCI DSS requirements** for protecting payment card data.

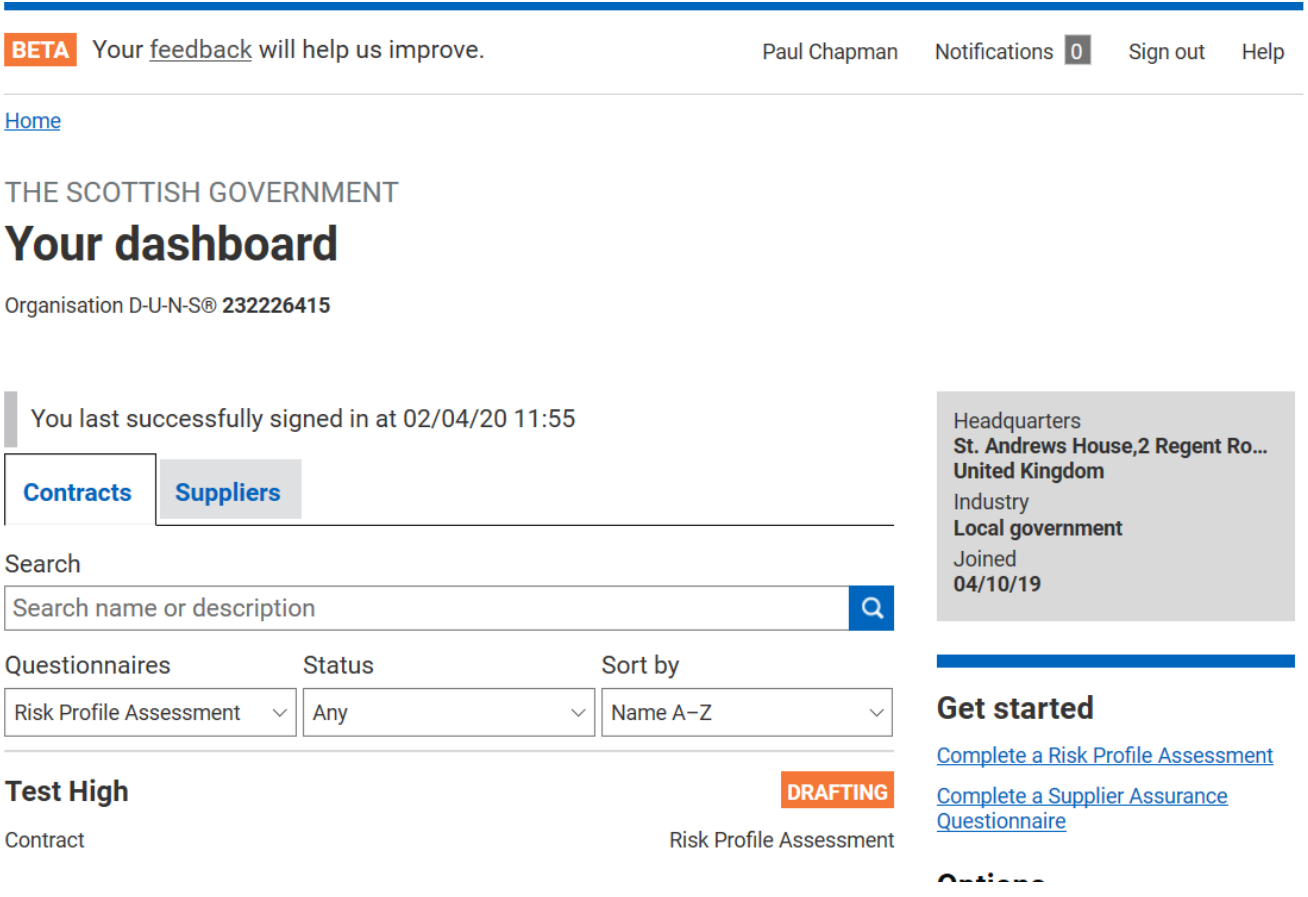
Scottish Cyber Assessment Service



Scottish Cyber Assessment Service



Scottish Cyber Assessment Service



Scottish Cyber Assessment Service

Supplier Assurance Questionnaire

This Supplier Assurance Questionnaire (SAQ) forms part of the Scottish Cyber Assessment Service (SCAS), a public sector tool for the improvement of cyber security in the supply chain.

It allows a supplier to demonstrate their compliance with the controls required for a contract's Cyber Risk Profile, as established by the contracting authority.

This assurance is provided by every bidding supplier.

Depending on the contract's risk profile and your organisation's certification status, completing a SCAS SAQ for the first time can take time and effort. It may take a number of hours for higher risk profile contracts, particularly if you are not familiar with your organisation's cyber security arrangements.

However, once complete, many of your answers can be re-used if you are bidding for other public sector contracts (provided the contracting authority is using SCAS). So it is worth taking the time to get your answers right.

If you hold certain certifications covering the full scope of the contract, this can also significantly reduce the number of questions you need to answer.

Completing a sample SAQ is also a cost-free way of better understanding how close you are to meeting the requirements of certain certifications.

Continue

Guidance

You are in the 'Introduction' section of this questionnaire.

This Supplier Assurance Questionnaire (SAQ) forms part of the Scottish Cyber Assessment Service (SCAS), a public sector tool for the improvement of cyber security in the supply chain.

Scottish Cyber Assessment Service

Supplier Assurance Questionnaire

Complete a Supplier Assurance Questionnaire

Before you start the Supplier Assurance Questionnaire, you will need to have knowledge of the cyber security arrangements for your organisation and any cloud-based or non-cloud based solutions/products to be supplied under this contract.

Depending on the contract's Cyber Risk Profile, you may need to have knowledge of your organisation's:

- relevant certifications held, and the extent to which they cover the scope of this contract
- information security policy
- sensitive information policy
- removable media policy
- information technology estate/network policies
- user access policies personnel checks and vetting policies
- incident reporting and management policies

If you will rely on cloud service providers to deliver any part of this contract, you will also need to provide information about those providers' security arrangements.

Guidance

You are in the 'Introduction' section of this questionnaire.

Continue Previous

Save and view answers

Scottish Cyber Assessment Service

Supplier Assurance Questionnaire

Public sector organisations and suppliers are encouraged to work together collaboratively to improve cyber security. **It is vitally important that you provide honest, frank answers to the questions in SCAS to help facilitate this approach.**

If the Contracting Authority has opted to accept Cyber Implementation Plans for this contract, non-compliance with the minimum cyber security requirements will not automatically result in bidders being excluded. You will have the opportunity to address any areas of non-compliance to timescales agreed with the Contracting Authority.

If you are successful in your bid for this contract, your answers to the SAQ will form part of the contractual terms and conditions for this contract. The contracting authority may require an audit of the cyber security arrangements for this contract under agreed contractual terms in order to assess compliance.

Continue Previous

Guidance

You are in the 'Introduction' section of this questionnaire.

Save and view answers

Scottish Cyber Assessment Service

Home > Your dashboard > Supplier Assurance Questionnaire - 1586265897

Supplier Assurance Questionnaire

SI1. Does your organisation have a Risk Profile Assessment Reference (RAR) to link to this questionnaire?

- ◯ Yes
  I have a reference and wish to link this SAQ to a Risk Profile Assessment now
- ◯ No
  I want to complete a sample SAQ to assess my capability

Guidance

You are in the 'Introduction' section of this questionnaire.

Scottish Cyber Assessment Service

Supplier Assurance Questionnaire

Important

Once you have completed the SAQ, SCAS will provide you with a **downloadable report** informing you whether you have met the cyber security requirements for this contract.

You should download the SAQ report and submit it along with all other tender bid documentation via the relevant portal (e.g. PCS, PCS-T) or method used by the contracting authority for this procurement.

Where necessary, you should use the report to support your development of a CIP in order to demonstrate that you will be able to meet requirements that you currently do not meet. A CIP must set out credible information on:

- the supplier's proposed actions to achieve the requirements it currently does not meet - this may include proposed alternative mitigations or controls to manage relevant cyber risks; and/or
- the supplier's reasoning as to why compliance with specific minimum requirements is not necessary for the contract; and
- in line with any requirements specified by the contracting authority in SCAS and Instructions to Tenderers, the date or contract phase by which the supplier intends to achieve the requirements or have in place alternative mitigations or controls.

The contracting authority should have supplied a template CIP along with all other ITT documentation. One can be downloaded here.

Guidance

You are in the 'Introduction' section of this questionnaire.

Continue Previous Save and view answers

Scottish Cyber Assessment Service

Home > Your dashboard > Supplier Assurance Questionnaire - 1586265897

Supplier Assurance Questionnaire

You are on page **1** of **10**

Do you want to re-use answers from an existing Supplier Assurance Questionnaire?

You can select an existing Supplier Assurance Questionnaire and re-use the answers.

This can help save time if you have previously completed an SAQ for a contract with the same (or similar) risk profile as this one.
NB: You must ensure that the auto-completed answers remain relevant to this specific contract.

Answers can be edited to reflect changes relevant for this contract, before it is submitted.

Re-use an existing Supplier Assurance Questionnaire

Continue

Guidance

You are in the 'General Contract Context' section of this questionnaire.

Scottish Cyber Assessment Service

Supplier Assurance Questionnaire

You are on page **5** of **12**

SI7. Will your proposals for the contract involve you delivering any other (non-cloud-based) digital products or solutions, for public sector organisations to install or configure to support the processing of information?

▼ Guidance

If you will be delivering non-cloud-based digital products or solutions that the public sector will install or configure to support the processing of information, you should ensure that you include consideration of the secure development environment for all such products or solutions when answering the SAQ questions.

In addition, you will be presented with some specific questions about the basic security features of the products/solutions you intend to supply. These questions will be presented after the main SAQ questions.

▼ Examples

Examples may include a server or database that will be connected to public sector networks, Internet of Things devices, a medical scanner that connects to health board systems, etc.

- ○ Yes
- ● No

Guidance

You are in the 'General Contract Context' section of this questionnaire.

Other options

Invite user to collaborate

Scottish Cyber Assessment Service

Certification

SI9. Please indicate whether you hold any of the following certifications or accreditations, covering the full scope of the contract. Tick all that apply.

- [ ] Cyber Essentials or equivalent
- [x] Cyber Essentials Plus or equivalent

  Provide Certification number

  Upload evidence of certification (pdf, image)

  Browse... | Browse previous...

  Saved attachments

  File name

  You haven't added any attachments

- [ ] IASME Governance Gold or equivalent
- [ ] ISO27001 or equivalent
- [x] None of the above

Continue | Previous

Guidance

You are in the 'General Contract Context' section of this questionnaire.

Please consider very carefully the extent to which any certifications held cover the entire scope of the solutions, products or services that you will rely on to deliver the contract. You will be asked to supply evidence of this, by submitting the relevant certification.

Where the certifications cover the entire scope of the contract, SCAS allows you to rely on those certifications to auto-complete answers in the Supplier Assurance Questionnaire.

It is your responsibility to confirm that all information supplied under the SAQ process is accurate.

Other options

Invite user to collaborate

Save and view answers

Scottish Cyber Assessment Service

You are on page **8** of **11**

Completing the SAQ

You will now be guided through a series of questions relating to the controls and security measures that your organisation has in place to protect delivery of the contract from cyber threats.

Important: Please ensure answers accurately describe **all digital networks and services** (including any third party cloud service providers your organisation relies on) that are relevant to the following aspects of this contract:

- the cyber security of information processed by your organisation (or its suppliers) which the public sector "owns" or is ultimately responsible for;
- the cyber security of any cloud-based products or solutions you are delivering to support the public sector's processing of information;
- the cyber security of the development environment for any products and solutions you are delivering to the public sector; and/or
- your ability to withstand and recover from cyber attacks to ensure service continuity.

If you are providing non-cloud digital products under this contract, questions about product security will be presented in a subsequent section of the SAQ.

All questions should be answered only as they relate to your specific proposals for delivery of the contract.

Guidance

You are in the 'SAQ' section questionnaire.

Continue Previous Save and view answers

Scottish Cyber Assessment Service

Supplier Assurance Questionnaire

You are on page **9** of **11**

SAQ173. Are the following measures in place to back up computer systems data? Tick all that apply.

► Small Business Guidance

- [ ] The data that needs to be backed up to keep relevant systems running and protect customer data and information has been identified.
- [ ] This data is backed up on a regular basis, and at least daily.
- [ ] Backups are kept safe and separate, so they cannot be hacked if someone manages to hack computers or systems related to the contract.
- [ ] Due consideration has been given to using cloud services for backups, where this may offer more resilience.
- [ ] None of the above
- [ ] Not applicable/alternative mitigations in place

SAQ174. Are the following measures in place to protect your systems from malware? Tick all that apply.

► Small Business Guidance

- [ ] Firewalls are used to protect relevant networks, and the built in firewalls on computers and laptops are switched on, especially if laptops are used outside of the office.
- [ ] Antivirus software is installed on all relevant computers and laptops, updated at least daily, and set to scan computers, anything that is

Guidance

You are in the 'Very Low assessment level' section of this questionnaire.

The minimum acceptable response for these questions is to tick at least 75% of the controls, that are applicable to your organisation.

Other options

Invite user to collaborate

Scottish Cyber Assessment Service

Submitting the SAQ

Thank you for completing the Supplier Assurance Questionnaire.

By submitting the SAQ, you are confirming that all answers provided in the response to this section of the SAQ are a true and accurate representation (where applicable) of:

- **all digital networks and services** (including any third party cloud sevice providers your organisation relies on) that are relevant to the following aspects of **this specific contract:**
  - the cyber security of information **processed by your organisation** which the public sector "owns" or is ultimately responsible for;
  - the cyber security of any **cloud-based products or solutions** you are delivering to support public sector processing of information;
  - the cyber security of the **development environment** for any **products and solutions** you are delivering to the public sector; and/or
  - your ability to withstand and recover from cyber attacks to ensure **service continuity**.
- **any non-cloud based digital products and solutions** that you will be providing under **this specific contract.**

You acknowledge that, if you are successful in your bid for this contract, your answers to the SAQ may form part of the contractual terms and conditions for this contract.

The contracting authority may require an audit of the cyber security arrangements for this contract under agreed contractual terms in order to assess compliance.

Guidance

You are in the 'Submitting SAQ' section of this questionnaire.

Continue Previous Save and view answers

Scottish Cyber Assessment Service

Supplier Assurance Questionnaire

You are on page **11** of **11**

Declaration

You are about to submit your answers. **Before doing so, please check your responses for accuracy**. To help do this, you can download a copy of your SAQ responses using the link below. The minimum acceptable answers for this contract's risk level are indicated by asterisks. Answers that have been automatically assumed based on certifications held by your organisation are set out in the certification annex.

If you need to make any changes following the review of your answers, **please click "Save and view answers" now and make the necessary changes in the SCAS tool before submitting your final answers.**

Pre-submission Copy of SAQ Answers
Document
Pre-submission Copy of SAQ Answers

Once you click "Submit", you will not be able to go and change your responses.

Please confirm the following statements:

- I have authority to complete the Supplier Assurance Questionnaire

Guidance

You are in the 'Submitting SAQ' section of this questionnaire.

Scottish Cyber Assessment Service

You are on page **11** of **11**

Declaration

You are about to submit your answers. **Before doing so, please check your responses for accuracy**. To help do this, you can download a copy of your SAQ responses using the link below. The minimum acceptable answers for this contract's risk level are indicated by asterisks. Answers that have been automatically assumed based on certifications held by your organisation are set out in the certification annex.

If you need to make any changes following the review of your answers, **please click "Save and view answers" now and make the necessary changes in the SCAS tool before submitting your final answers.**

Pre-submission Copy of SAQ Answers
Document
Pre-submission Copy of SAQ Answers

Once you click "Submit", you will not be able to go and change your responses.

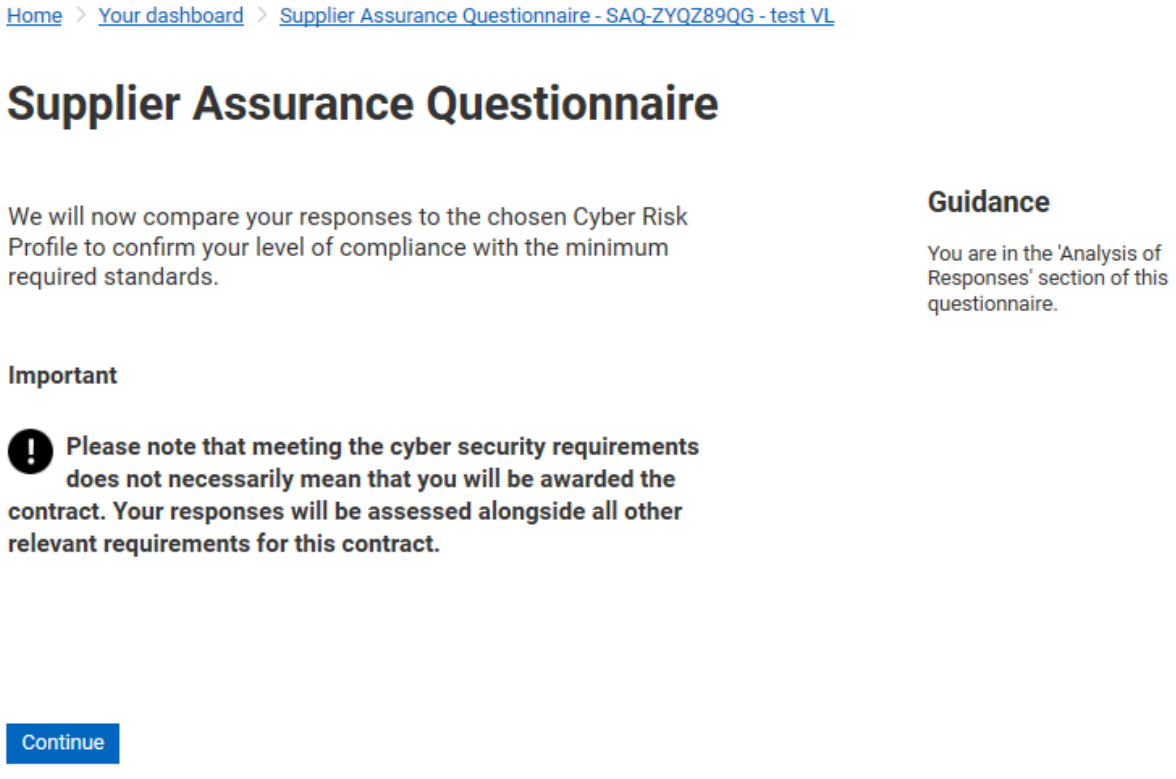
Please confirm the following statements:

- 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 actions to notify the contracting authority

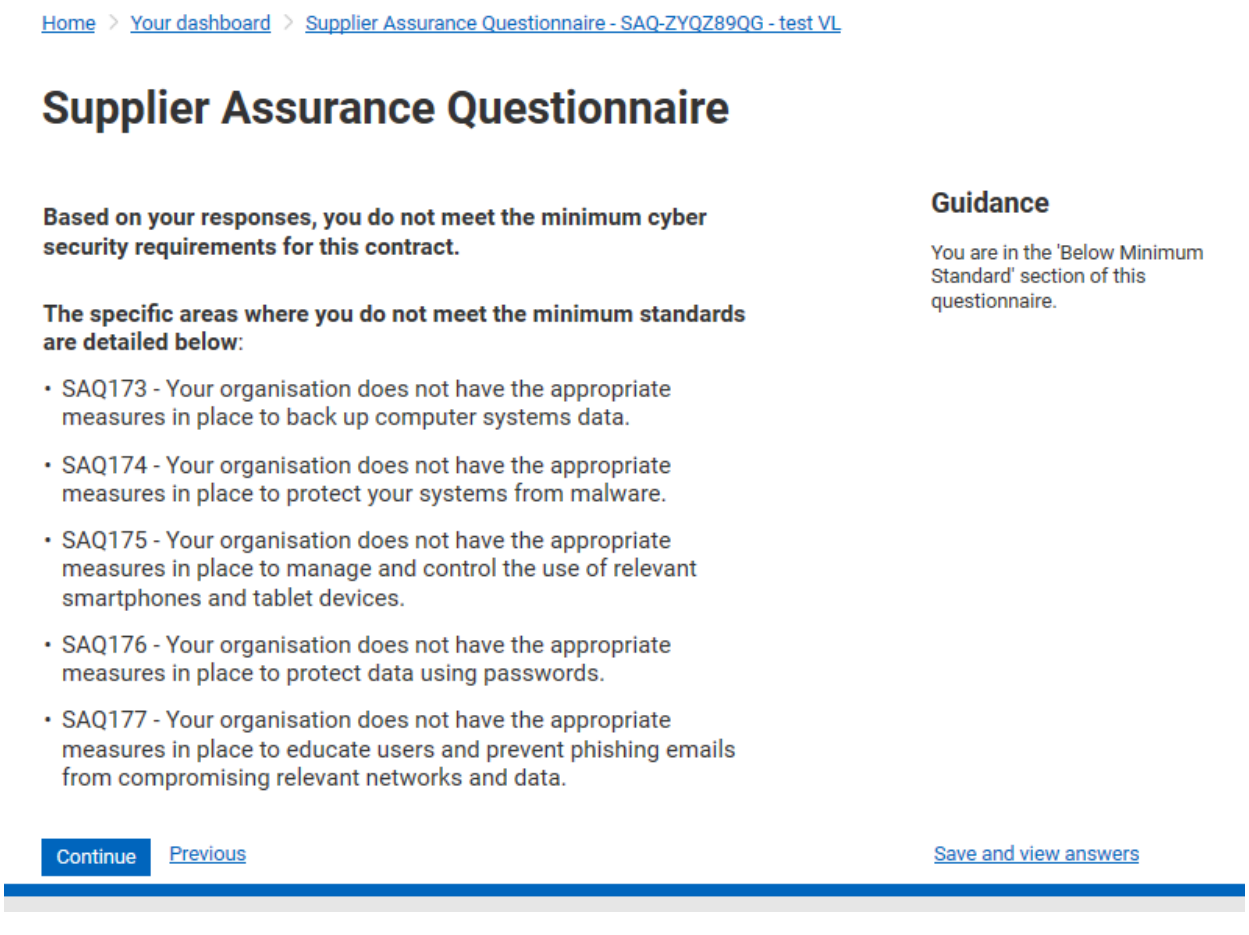
Guidance

You are in the 'Submitting SAQ' section of this questionnaire.

Scottish Cyber Assessment Service



Scottish Cyber Assessment Service



Scottish Cyber Assessment Service

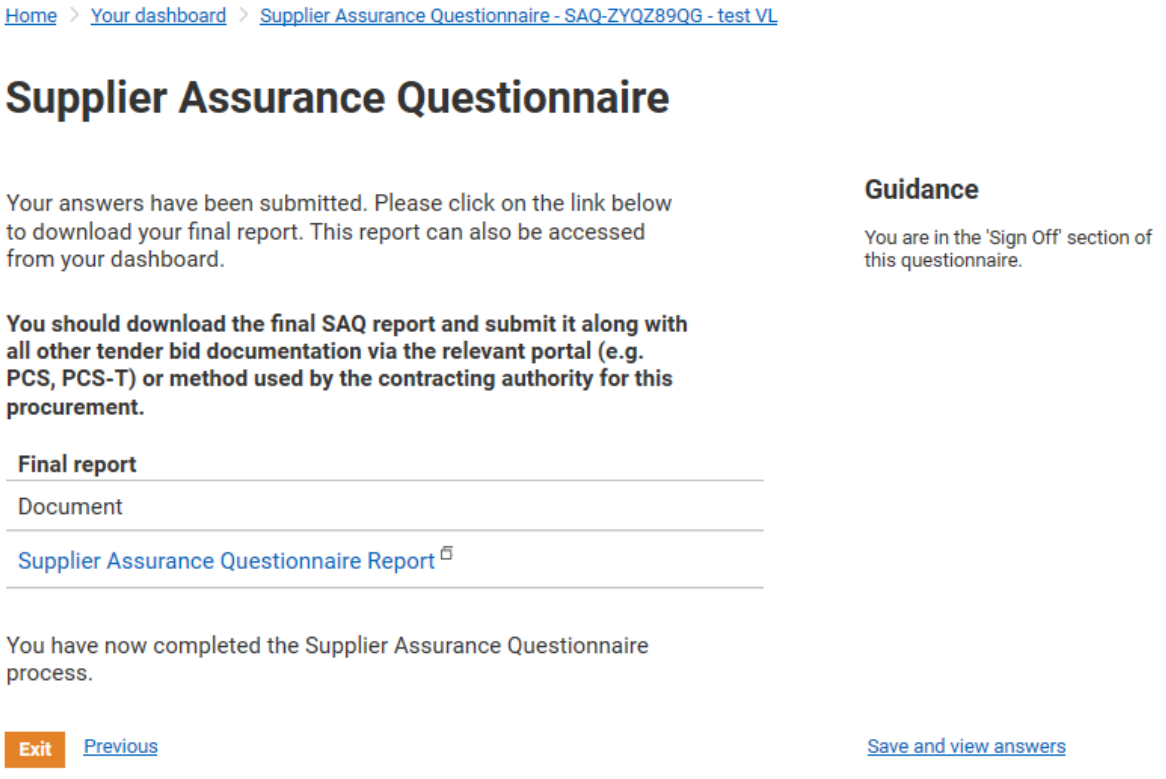
CYBER IMPLEMENTATION PLAN – TEMPLATE FORM

CYBER IMPLEMENTATION PLAN	
CONTRACT DETAILS	
1. Contract title	
2. Contract number	
3. Unique SCAS Cyber Risk Assessment Reference number	
4. SCAS Cyber Risk Profile	
5. Name of supplier, and details of authorised officer completing this CIP	
PROPOSED APPROACH TO AREAS WHERE MINIMUM BENCHMARK REQUIREMENTS ARE NOT CURRENTLY MET	
6. Using the feedback from the SCAS SAQ Report, please provide: (i) details of areas where your organisation does not currently meet the benchmark minimum requirements for this contract; and	

51

(ii) for each such area identified, details of the actions you intend to take to achieve the minimum benchmark requirements, OR the alternative mitigations or controls you have in place, OR your reasoning as to why compliance with the minimum benchmark requirements is not necessary for this contract.				
Details of minimum benchmark requirements not currently met *Please refer to the feedback in your SCAS SAQ Report in order to complete this section.*	Supplier's alternative mitigations (effective from contract commencement)	Supplier's reasoning as to why compliance is unnecessary for this contract.	Supplier's proposed further action (to be implemented during the contract)	By which date(s) do you undertake to have implemented such further action?
[Insert details here]				
[Delete this row if not required]				

Scottish Cyber Assessment Service



Scottish Cyber Assessment Service

Organisation Name:
CORE WORKING GROUP

Scottish Cyber Assessment Service

SUPPLIER ASSURANCE QUESTIONNAIRE

Supplier Assurance Questionnaire Reference: SAQ-V5AX88G3

Connected Risk Assessment Reference: RAR-74952TET

Instructions for submission

Please follow any special instructions for submission of your SAQ from your contracting authority. In normal circumstances, the procedure is as follows:

1. Download and/or print off this SAQ report from the Scottish Cyber Assessment Service tool.

2. If required, use the information contained in the report to complete a Cyber Implementation Plan.

3. Submit both this SAQ report and any completed Cyber Implementation Plan along with all other tender documents, via the relevant portal (e.g. PCS or PCS-T) or other method preferred by your contracting authority.

Scottish Cyber Assessment Service

Your Performance

Your performance against the SCAS model is assessed by comparing the Cyber Risk Profile against your SAQ score. The comparison determines whether you have met the requirements of the Cyber Risk Profile and therefore whether you are compliant with the SCAS model, and eligible for the relevant contract.

Overview

Section Title	Minimum Compliance	Overall Performance
Governance	Compliant	-0% Green +100% -100% Assurance +100%
Risk Management	Non-compliant	-100% Red +0% -100% Assurance +100%
Asset Management	Compliant	-0% Green +100% -100% Assurance +100%
Personnel Security	Compliant	-0% Green +100% -100% Assurance +100%
Access Management	Compliant	-0% Green +100% -100% Assurance +100%

Below Minimum Standard 1 question

Based on your answers, you have not sufficiently met the minimum standard as defined by the Cyber Risk Profile for this contract.

- SAQ6 - Your organisation does not have a risk management regime consisting of ICT risk assessment and management processes, which assess the risks to relevant information and systems, using a repeatable formal assessment process or at minimum on an ad hoc basis.
- SAQ8 - Your organisation has not ensured senior management review the effectiveness of the information security programme on a regular basis.

Scottish Cyber Assessment Service

Guidance and support

- Procurement Journey and Supplier Journey being updated to reflect these developments.
- Full suite of guidance in place (inc. Supplier comms toolkit), available via different routes (Supplier Journey, Procurement Journey, Gov.Scot, SCAS tool, etc).
- Support package in place for SMEs and charities, signposted from key sources:
    - ~~Cyber Essentials voucher scheme~~
    - Digital Development Loans (https://digitaldevelopmentloan.org/)
    - Digital Boost Scheme (https://www.bgateway.com/resources/digitalboost)

Scottish Cyber Assessment Service

Further Information:-

- Cyber Resilience Framework – Applies to Scottish Public Sector organisations and encourages robust management of supply chain cyber security.
- Scottish Procurement Policy Note (SPPN 2/2020) – Public Sector Supplier Cyber Security Guidance
- Scottish Public Sector Supplier Cyber Security Guidance Note
  - Supporting Documentation (Example Tender wording, contract clauses, Cyber Implementation Plan Template, Question Sets & communications resources).
- Scottish Cyber Assessment Service Tool – available for public sector organisations as buyers and all private sector organisations as suppliers.

Questions?

Paul.chapman@gov.scot

Paul Chapman

Head of Public Sector Cyber Resilience

Scottish Government
Riaghaltas na h-Alba
gov.scot