Scottish Cyber Assessment Service

Paul Chapman, Head of Public Sector Cyber Resilience
paul.chapman@gov.scot

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 businesses and charities often ask: “Why would anyone attack me?”

But if you rely on Internet-connected digital services or products to deliver your business objectives, **you are at risk**.

The Cyber Threat

- Many cyber attacks are **untargeted**

- Cyber attackers may never have heard of your business or organisation until the day they manage to get access to your networks.

- The Scottish Government believes that it is vital for all businesses and charities in Scotland understand the cyber threat and prepare to take action to mitigate it.

The Supply Chain Cyber Threat

- You may be targeted as a route to larger organisations

The Scottish public sector wants to ensure its suppliers have appropriate cyber security in place as:

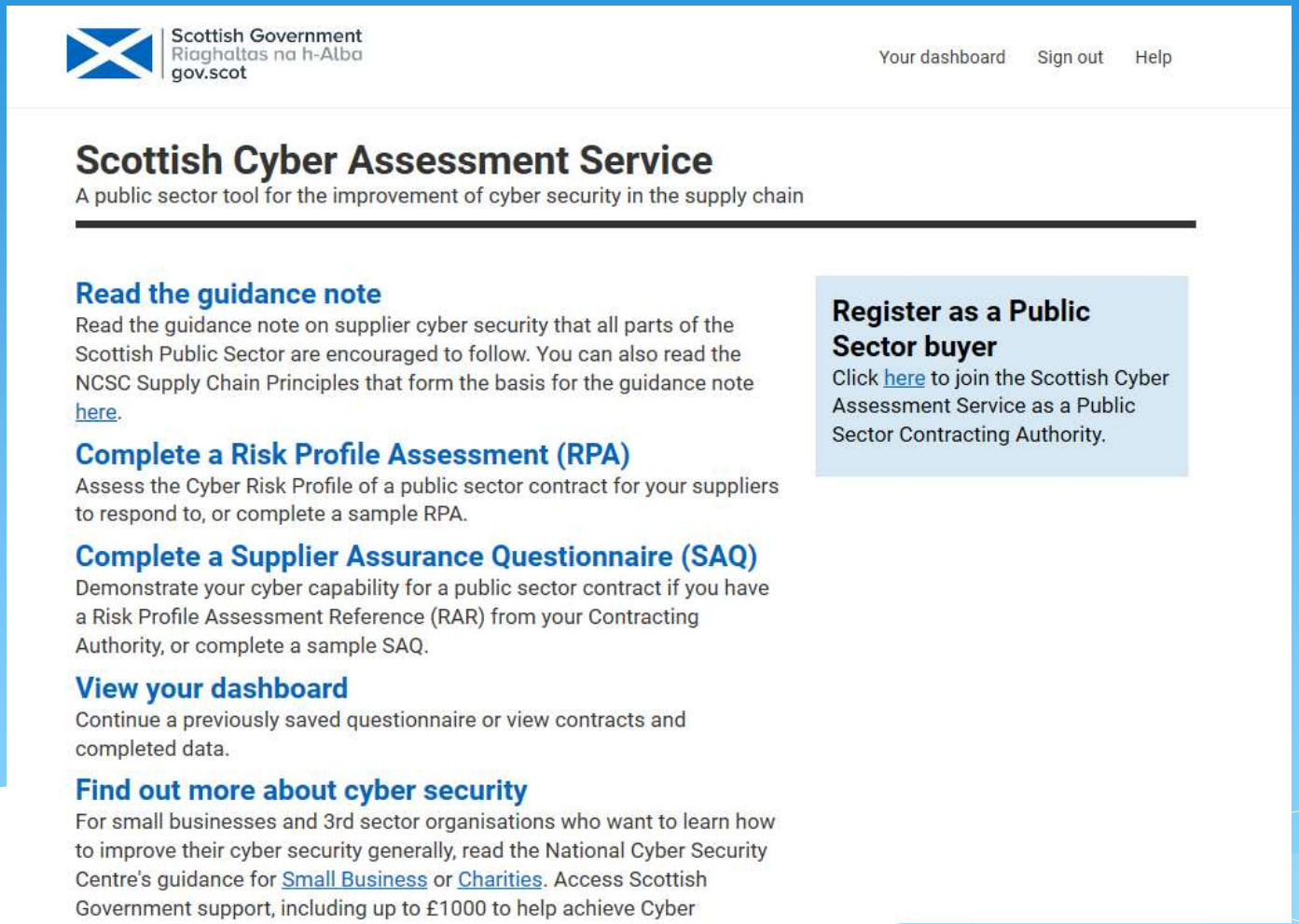
- We have a duty to prevent public services from being disrupted; and

- We want to support our suppliers to improve their cyber security, because it's good for the sustainability and resilience of our digital economy and wider society.

The Scottish Cyber Assessment Service

- A more consistent approach to supply chain security.
- A **guidance note**, which has been produced for all public sector organisations, setting out best practice from the National Cyber Security Centre
- A support tool called the **Scottish Cyber Assessment Service**, which all suppliers bidding for public sector contracts may be asked to use.

Scottish Cyber Assessment Service



Scottish Government
Riaghaltas na h-Alba
gov.scot

Scottish Cyber Assessment Service

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

- Public sector organisations will use the tool to complete a **Cyber Risk Profile Assessment** for all 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.

- All suppliers bidding for a contract will then be given a **Risk Assessment Reference**. They can use this to log onto the Tool, complete the relevant Supplier Assurance Questionnaire, and download a report to submit alongside all other tender documents.

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

- Public sector organisations will then assess the answers provided as part of their evaluation of tenders.

- The tool helps to manage supplier burdens in two main ways:

    - Consistent questions for similar contracts across the public sector
    - Suppliers can reuse many/all of the answers they have supplied previously

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.

Public sector buyer uses Risk Profile Assessment Tool to generate risk profile.

Supplier presented with Supplier Assurance Questionnaire aligned to risk profile.

Certification options

Cyber risk profile assessment

HIGH RISK PROFILE	*Advanced approaches to cyber resilience, most likely to be appropriate for organisations facing sophisticated threats with high potential impact.*	NIS + ISO
MODERATE RISK PROFILE	*Holistic approaches to cyber resilience, provide greater assurance that targeted attacks can be resisted or dealt with when they occur.*	NCSC 10 Steps + GDPR controls
LOW RISK PROFILE	*Controls for Very Low risk profile PLUS Cyber Essentials*	Basic Controls + Controls from Cyber Essentials
VERY LOW RISK PROFILE	*Very low risk profile*	Basic Controls aligned with NCSC Small Business Guide
N/A – No cyber risk identified in contract.	*Public bodies encouraged to signpost suppliers to good practice*	Signpost suppliers to good practice e.g. NCSC Guidance

Specialist requirements (e.g. List X, etc.)

Progressively more holistic cyber resilience measures

CiSP

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

Incident reporting

Organisations are required to 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

What if a supplier doesn't currently meet the requirements of a contract's risk profile? Are they excluded from bidding?

- The Guidance Note and SCAS are designed to encourage a **proportionate approach** to supply chain cyber security.

- This includes an ability for public sector organisations to opt not to exclude suppliers that do not meet a SCAS risk profile's minimum requirements at the time of bidding.

- In such circumstances, they can opt to accept an accompanying **Cyber Implementation Plan**, in which the supplier commits to achieving the minimum requirements by a specified future date (e.g. contract award).

Cyber Resilience Unit

cyberresilience@gov.scot

Scottish Government
Riaghaltas na h-Alba
gov.scot