

CivTech 9 – Challenge 9.5: Additional Information discussed at the Q&A.

How can we use technology to create the most efficient and secure supply chain for public sector procurements?

Cyber Security, Design Standard and Design System

Cyber Security

The current Cyber Security Procurement Support Tool has been in place for over 3 years. It sits on our supplier platform but the question set and risk assessment processes are Scottish Government IP - guidance and questions set spreadsheet can be found here - <https://www.gov.scot/publications/cyber-resilience-supply-chain-guidance/> .

The CSPST was developed to address the challenges that the public sector bodies had in applying NCSC's Supply Chain Security Guidance during procurement , to address the lack of consistency in assurance practices across the sector and to try to reduce the burden on both suppliers and buyers by allowing reuse of questions and answers.

The CSPST is used by Scottish public sector buyers to risk assess potential contracts at the outset of a procurement with the assessment being issued as part of the ITT. Different bodies use the tool in different ways with the assessment being carried out by cyber/information security teams, procurement professional and/or policy managers.

Suppliers can come our CSPST and answer the relevant questions using a reference number supplied in the ITT. They complete their Supplier Assurance Questionnaire, download their compliance report and submit it along with their bid for the contract for evaluation by the buyer. The Supplier can reuse their answers between different contracts with similar risk profiles.

However, the sector has evolved, as have the wider considerations in procurement processes and crucially the cyber/information security challenges faced have also evolved. Cyber assurance is no longer just a consideration at the point of procurement but must be periodically revisited throughout the life of a contract, and at a frequency proportionate to the criticality of the contract. The current tool is not designed to support this function.

The existing CSPST can be accessed at <https://cyberassessment.gov.scot/> and the current user experience can be tested by registering as a buyer, competing a Supplier Assurance Questionnaire and choosing to answer a sample one.

You can choose the Risk Profile level you'd like to answer – Low, Moderate or High for questions broadly extrapolated from Cyber Essentials, NCSC 10 Steps to Cyber Security/GDPR Technical Requirements and NIS CAF/ISO27001 respectively).

CSPST System Statistics, as at 30 June 2023

	Registered and Active	Registered Users	Average Usage Per Month in 2023
Scottish Public Sector Bodies	83	546	21 Contracts risk assessed
Supplier Organisations	910	1193	39 Supplier Assurance Questionnaires completed
Totals	993	1,739	

Digital Scotland Service Standard

The service standard aims to make sure that services in Scotland are continually improving and that users are always the focus.

<https://www.gov.scot/publications/digital-scotland-service-standard/>

Digital Scotland Design System

The Digital Scotland Design System provides static web assets for websites and web applications for the Scottish Government and other Scottish public sector bodies.

The Design System is open source and free to use.

<https://designsystem.gov.scot/>