



### **Cyber Resilience – Public Sector Action Plan – Cyber Resilience Framework & Supply Chain Cyber Security Guidance**

**Committee**            Audit and Standards

**Date of meeting**    14 February 2020

**Date of report**    24 January 2020

**Report by Assistant Chief Executive**

#### **1. Object of report**

To advise the committee on the publication of the Scottish Public Sector Cyber Resilience Framework and Supply Chain Cyber Security Guidance Note from the Scottish Government and SPT's position as at February 2020.

#### **2. Background**

##### Letter from Deputy First Minister and Cabinet Secretary for Education and Skills

On 20 January 2020, the Deputy First Minister and Cabinet Secretary for Education and Skills wrote to the Chief Executive to inform of the publication of the Scottish Public Sector Cyber Resilience Framework and Supply Chain Cyber Security Guidance (see attached).

##### The Cyber Resilience Framework (the Framework)

The key aims of the Framework are to *'provide a common, consistent reference point for the Scottish public sector to inform decision-making about cyber resilience. It is also expected to provide an effective, commonly accepted basis for external audit and inspection activities.'*

The letter states that SPT is *'requested to report (annually) on progress on implementation of the Framework from July 2020 to 2021.'*

##### Scottish Public Sector Supplier Cyber Security Guidance Note (the Guidance Note)

The letter states that *'legislative requirements, including the General Data Protection Regulation (GDPR), require all public sector organisations to ensure appropriate technical protections are in place when suppliers process personal data.'*

The letter adds that *'all public sector organisations are asked to update their procurement processes to align with the Guidance Note as soon as possible and in any case in readiness for the start of the next financial year.'*

### 3. Outline of SPT’s position as at February 2020

#### Cyber Resilience Framework diagram

The following diagram outlines the Scottish Public Sector Cyber Resilience Framework objectives.



### SPT position as at February 2020 – Cyber Resilience Framework

With reference to the above diagram and objectives, SPT's position is as follows:

**Initial baseline** – CE+ accreditation was achieved by October 2018 and maintained in 2019;

**Target** – GDPR implementation and PCI-DSS has been achieved and is on-going.

**Advanced** – Alignment with the Security of Network and Information Systems (NIS) requirements and resource implications is subject to review.

### SPT position as at February 2020 – Supplier Cyber Security Guidance Note

SPT's procurement processes utilise Scottish Government frameworks and contract award documentation includes a cyber-security clause.

The requirements of the Guidance Note and resource implications are subject to review for implementation in accordance with the prescribed timescale.

## 4. Committee action

The committee is asked to note the contents of this report and the letter from the Deputy First Minister and Cabinet Secretary for Education and Skills dated 20 January 2020.

## 5. Consequences

Policy consequences	<i>In accordance with the Information Security Policy.</i>
Legal consequences	<i>None directly.</i>
Financial consequences	<i>The resources required to implement the Framework will be met from SPT's capital and revenue budgets.</i>
Personnel consequences	<i>None directly.</i>
Equalities consequences	<i>None directly.</i>
Risk consequences	<i>As detailed in the report.</i>

**Name** Valerie Davidson

**Name** Gordon MacLennan

**Title** Assistant Chief Executive

**Title** Chief Executive

For further information, please contact Neil Wylie, Director of Finance on 0141 333 3380.

F/T: 0300 244 4000  
E: [dfmcse@gov.scot](mailto:dfmcse@gov.scot)

*[Chief Executive / Principals / Commissioners of  
public sector organisations]*

20 January 2020

Dear *Chief Executive / Principal / Commissioner*,

## **Cyber Resilience – Public Sector Action Plan – Cyber Resilience Framework & Supply Chain Cyber Security Guidance**

Following my earlier correspondence in relation to the Public Sector Action Plan on cyber resilience, I am writing to inform you that the Scottish Public Sector Cyber Resilience Framework and Supply Chain Cyber Security Guidance have now been published. These can be accessed, along with detailed guidance on their use and their support tools, on the Scottish Government website (References <sup>1</sup> and <sup>2</sup> in the footnotes).

I trust you will find the Framework, its accompanying self-assessment tool and Supply Chain Cyber Security Guidance useful when considering your cyber resilience arrangements in the context of your business risks.

### **The Framework**

To help Scotland's public sector continue its journey towards levels of cyber resilience that are proportionate to the threat faced, and in response to feedback about the difficulties public sector organisations face in understanding and interpreting the plethora of cyber security standards currently in use, the Public Sector Action Plan committed us to developing a Scottish Public Sector Cyber Resilience Framework.

The key aims of the Framework are to provide a common, consistent reference point for the Scottish public sector to inform decision-making about cyber resilience. It is also expected to provide an effective, commonly accepted basis for external and internal audit and inspection activities.

---

<sup>1</sup> <https://www.gov.scot/publications/cyber-resilience-framework>

<sup>2</sup> <https://www.gov.scot/publications/cyber-resilience-supply-chain-guidance/>

Scottish Ministers, special advisers and the Permanent Secretary are covered by the terms of the Lobbying (Scotland) Act 2016. See [www.lobbying.scot](http://www.lobbying.scot)

For organisations that are currently required to work to individual standards, such as Cyber Essentials, Public Services Network(PSN), ISO 27001 or the Security of Network and Information Systems (NIS) Regulations, the Framework has been designed to provide a way of understanding levels of compliance with these standards in addition to a range of other key standards that your organisation, or partner organisations in the public, private or third sectors, may be required or requested to report against. Adopting the Framework is therefore expected to help promote greater alignment and trust between Scottish public sector organisations and, in some circumstances, private and third sector partners, over time – a vitally important goal given the increasing need to collaborate and share data across all sectors to deliver quality services to Scotland’s economy and society.

### **The self-assessment tool**

To support effective implementation of the Framework, the Scottish Government has worked with a supplier to produce a concept cyber resilience self-assessment tool. This basic tool is intended to support the production of information for key audiences within public sector organisations, helping them to identify broad areas of strength and weakness and levels of compliance against the Framework and individual standards.

It is our intention to develop this into a more sophisticated, database-driven tool in due course, with improved functionality and the ability to produce reports for different internal and external audiences, including senior level executives and external auditors/regulators. This work, which will include burden reduction as a key focus, will be taken forward for launch during the next financial year.

### **Implementation**

The Scottish Government’s proposed approach to implementation and reporting arrangements for the Framework is as follows:

- **January 2020 to end June 2020:** a “soft launch” period, allowing public sector organisations to familiarise themselves with the Framework and adjust processes and funding arrangements to support appropriate implementation.
- **July 2020 to 2021:** full implementation, under which public sector organisations will be requested to report regularly (annually) on progress against the Framework. Its requirements will be included in the Scottish Public Finance Manual. Audit bodies will be encouraged and supported to align their activities with the Framework where they feel this is appropriate. The full version of the self-assessment tool will be launched in order to help alleviate reporting burdens and support effective implementation during this phase.

### **Resources and available support**

I recognise that implementation of the Framework may involve resource burdens for public sector organisations. The Scottish Government believes it is important that all organisations view the costs of appropriate cyber resilience as a fundamental part of the overall cost of digital public services. Building consideration of cyber resilience into wider digital budgets is one potential way to support this cultural change.

More broadly, the Framework makes clear that it is intended for implementation on a **risk-based and proportionate basis**. Unless required by regulation or external bodies, it is for individual public sector organisations to judge whether to prioritise resources to implement specific aspects of the Framework in order to address risks, or to live with those risks. The

Scottish Ministers, special advisers and the Permanent Secretary are covered by the terms of the Lobbying (Scotland) Act 2016. See [www.lobbying.scot](http://www.lobbying.scot)

St Andrew’s House, Regent Road, Edinburgh EH1 3DG  
[www.gov.scot](http://www.gov.scot)



INVESTORS  
IN PEOPLE

Accredited  
Until 2020





Framework and assessment tool encourage organisations to note the reasons for such decisions for audit purposes.

A number of free resources have been made available from the Scottish Government to support implementation of key aspects of the framework. These include the self-assessment tool, the already-distributed funding for Cyber Essentials pre-assessments as part of the Public Sector Action Plan, publication of a free Training Guide, development of free Cyber Incident Response Plans and playbooks, and development of the Scottish Cyber Assessment Service to support decision-making around supplier cyber security. The Framework also includes links to relevant free NCSC guidance and tools.

I have asked my officials to monitor and assess any challenges the public sector faces in implementing the Framework during its first year, and to consider the potential for further targeted support to address shared challenges moving forward.

## **Supplier Cyber Security Guidance Note and Scottish Cyber Assessment Service Tool**

A key requirement in the Framework is for public sector organisations to manage the cyber resilience of their suppliers on a risk-based and proportionate basis. This commitment is vitally important for the protection of public services. There is an increasing trend for cyber criminals and hostile states to target “weak links” in supply chains in order to attack primary target organisations. Suppliers’ services can also be disrupted by “commodity” attacks that indiscriminately attack vulnerable networks via the Internet.

Legislative requirements, including the General Data Protection Regulation (GDPR), require all public sector organisations to ensure appropriate technical protections are in place when suppliers process personal data on our behalf. The Security of Network and Information Systems (NIS) Directive also specifically requires Operators of Essential Services in our devolved health and water sectors to have appropriate supply chain cyber security requirements in place.

To assist with this, in response to feedback from the Scottish public sector, the Scottish Government has worked with Procurement Centres of Excellence and other key partners to develop:

- A **Guidance Note on Supplier Cyber Security**. This recommends that public sector organisations adopt the National Cyber Security Centre’s supply chain guidance as the basis for their approach to supplier cyber resilience. The guidance note is available on the Scottish Government website<sup>3</sup>. An accompanying [Scottish Procurement Policy Notice<sup>4</sup>](#) will be published shortly.
- A decision-making support tool called the **Scottish Cyber Assessment Service (SCAS) Tool<sup>5</sup>**. This is available for optional use as an “open beta”<sup>6</sup>, and will be updated and improved after 6 months following feedback. It supports public sector organisations to

<sup>3</sup> <https://www.gov.scot/publications/cyber-resilience-supply-chain-guidance/>

<sup>4</sup> <https://www.gov.scot/collections/scottish-procurement-policy-notes-sppns/>

<sup>5</sup> <https://cyberassessment.gov.scot/>

<sup>6</sup> This means it is available for general use in a “live environment”, to allow for the gathering of feedback to improve performance.

Scottish Ministers, special advisers and the Permanent Secretary are covered by the terms of the Lobbying (Scotland) Act 2016. See [www.lobbying.scot](http://www.lobbying.scot)

assess cyber risks in contracts in a consistent way, and to place cyber resilience requirements on suppliers on a risk-based and proportionate basis; and

- A suite of supporting guidance and presentations available on the Scottish Government Cyber Resilience webpages<sup>7</sup>. These cover how to use SCAS in procurement processes, a Supplier Communications Toolkit and presentations for procurement officials and suppliers. Further support material and activities will be made available through the Supplier Development Programme in due course.

### **Key Recommended Actions for Your Organisation**

As you know, it is vitally important that cyber resilience is viewed as a business risk for your organisation and managed appropriately by your senior team. As a matter of good practice, this should include regular Board/senior-level consideration of supplier cyber risks and assurance activities around their mitigation.

I would be grateful if you would ensure that your organisation's senior Board/executive representative with responsibility for cyber resilience is made aware of the above support resources. These should also be brought to the attention of other key parts of your organisation, particularly those with procurement and cyber security expertise who may be responsible for implementing them.

All public sector organisations are asked to update their procurement processes to align with the Guidance Note (if necessary) as soon as possible, and in any case in readiness for the start of the next financial year.

Scottish Government standard terms and conditions have been updated to strengthen cyber resilience requirements, and to cater for optional use of the SCAS tool. Example wording for Contract Notices and ITTs when using SCAS is included in the SCAS guidance.

The NCSC Principles make clear the importance of communicating with suppliers and working in partnership to strengthen cyber resilience. To assist your organisation with this, and to help promote the support available from the Scottish Government and Supplier Development Programme, a Supplier Communications Toolkit has been produced. Your procurement and communications teams (where available) are encouraged to make use of this.

---

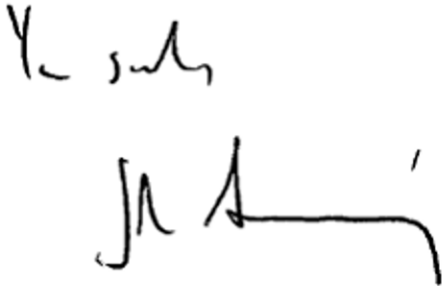
<sup>7</sup> <https://www.gov.scot/publications/cyber-resilience-supply-chain-guidance/>

Scottish Ministers, special advisers and the Permanent Secretary are covered by the terms of the Lobbying (Scotland) Act 2016. See [www.lobbying.scot](http://www.lobbying.scot)

## Feedback

My officials stand ready to offer support and advice on implementation of both the framework, the Supply Chain Cyber Security Guidance and their associated tools. We would welcome feedback in due course, to help improve both over time. Please send all questions and feedback to the Cyber Resilience Unit at [cyberresilience@gov.scot](mailto:cyberresilience@gov.scot).

Finally, I would like to offer you my sincere thanks for prioritising this work. I look forward to our organisations continuing to work constructively together to ensure that Scotland's public sector is leading by example in our drive to become a cyber resilient nation.

Handwritten signature of John Swinney in black ink.

**JOHN SWINNEY**

Scottish Ministers, special advisers and the Permanent Secretary are covered by the terms of the Lobbying (Scotland) Act 2016. See [www.lobbying.scot](http://www.lobbying.scot)

St Andrew's House, Regent Road, Edinburgh EH1 3DG  
[www.gov.scot](http://www.gov.scot)