Committee report

Cyber Resilience Framework update

Committee Audit and Standards

Date of meeting 19 February 2021 **Date of report** 26 January 2021

Report by Assistant Chief Executive

1. Object of report

To update the committee on the progress of implementation of the Scottish Public Sector Cyber Resilience Framework.

2. Background

From the initial overview report, presented to the Audit and Standards committee on 14 February 2020, members will recall, the Deputy First Minister and Cabinet Secretary for Education and Skills wrote to the Chief Executive to advice of the publication of the Scottish Public Sector Cyber Resilience Framework (the Framework), together with the expected reporting deadlines.

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 Framework contains four overarching domains, each with three progression stages from the core cyber standards.

The four overarching domains and their related categories are:

Manage security risk: this domain covers the organisational structures, policies and processes necessary to understand, assess and systematically manage security risks to Scottish public sector organisations' network and information systems and essential services;

Protect against cyber-attack: this domain covers the requirement for proportionate security measures to be in place to protect Scottish public sector organisations (and their essential services and systems) from cyber-attack;

Detect cyber security events: this domain covers measures to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, Scottish public sector organisations (and their essential services and systems);

Respond and **Recover**: this domain covers measures to minimise the impact of a cyber-security incident on Scottish public sector organisations (and their essential services and systems), including the restoration of services where necessary.

Progression stages

Within and across the four domains, the Framework sets out three progression stages. These represent progressive levels of sophistication so that, within each domain, public sector organisations are either required (i.e. by legislation) or can opt to implement basic, intermediate and more advanced sets of controls according to their sector and risk appetite.

Baseline: this is the progression stage that all Scottish public sector organisations are expected to achieve. It encompasses the requirements of the Scottish Public Sector Action Plan on Cyber Resilience, which itself encompasses a requirement to have independent assurance of the critical technical controls set out in the Cyber Essentials standard. If implemented appropriately, the requirements set out at the initial baseline stage should help mitigate against many of the most common internet-borne cyber threats.

Target: this is the progression stage beyond the initial baseline stage that all Scottish public sector organisations will be required or encouraged to achieve, on a risk-based and proportionate basis. It is effectively intended to be the new 'baseline' for public sector organisations. It encompasses the combined additional (i.e. beyond the initial baseline stage) requirements of General Data Protection Regulations (GDPR) and Payment Card Industry Data Security Standards (PCI-DSS). The requirements set out at the Target stage, if met, should generally help Scottish public sector organisations mitigate against more technically capable cyber-attacks.

Advanced: this is the progression stage that Scottish public sector organisations facing the most advanced cyber or network and information security threats, or those providing the most essential public services, will be required or encouraged to meet on a risk-based and proportionate basis. The advanced stage also represents a pathway beyond compliance for those public bodies that wish to move beyond the requirements of the target progression stage in specific areas, making clear what more can be done by Scottish public sector organisations that wish to become exemplars in the area of cyber resilience, or that wish to strengthen specific aspects of their cyber resilience arrangements. It is intended to encompass the combined additional (i.e. beyond the initial baseline and target stages) requirements of the Security of Network and Information Systems Directive (NIS).

The requirements set out at the Advanced stage, if met, should generally help mitigate against more advanced and persistent threats of the type that Scottish public sector organisations delivering the most essential services, or processing the most sensitive or valuable data, might reasonably be expected to face.

3. Progress to date

Committee has previously considered reports relative to cyber security arrangements within SPT, (meetings on 14 February 2020 and 28 August 2020)

The paper presented to the 28 August 2020 meeting outlined the initial self-assessment outcome which was completed following an assessment and input provided by a range of affected SPT services including the Digital team, Facilities, HR and Information Governance services and senior management.

The initial self-assessment as at August 2020 showed an overall compliance percentage of 73%

Note: progression towards a higher implementation rate may require additional resource allocation.

At this meeting, members agreed that the Director of Finance presents a further update report on the Cyber Resilience Framework in 2021, noting that the Chair requested regular updates on progress of the framework actions.

From the initial self-assessment, an action log was compiled for further management review. Each action was evaluated and risk-assessed. The review process assigned a lead officer(s) and a timescale for completion. Progress on the framework actions is monitored at a senior level on a 4 weekly basis thus ensuring progress is on track and is documented. In addition and to complement this work stream; the following management actions have been taken or are planned:

- Increased staff communications including intranet articles and emails to all staff and members on cyber threats with signposting to National Cyber Security Centre (NCSC) training resources;
- Specialised training on cyber security undertaken by Digital staff;
- External assessment of the digital security environment (penetration testing) and a review of the SPT security environment;
- Internal training sessions provided to digital system administrators;
- A refresh/refocusing of digital data cleansing throughout SPT services;
- Development and implementation of secure contactless payments at Bus and Subway stations, thus full PCI DSS compliance; and
- Recruitment of a Cyber security and continuity lead officer.

A further (second) self-assessment, concentrating on those areas previously identified as needing enhancement, has been provisionally scheduled for Q1 of 2021/2022 in order to action, develop and embed initiatives identified in the initial assessment. The findings will then be collated and presented to committee.

4. Committee action

The committee is asked to:

i. note the contents of this report;

ii. note the update on progress to meet the Cyber Resilience Framework requirements;

iii. agree that the Director of Finance presents a further update report on the Cyber Resilience Framework in August 2021.

5. Consequences

Policy consequences	*In accordance with the Information Security Policy.*
Legal consequences	*None directly.*
Financial consequences	*The resources required to implement the Cyber Resilience Framework will be met from SPT's capital and revenue budgets.*
Personnel consequences	*None directly.*
Equalities consequences	*None directly.*

Risk consequences	*Cyber resilience arrangements reduce the impact of cyber risks.*

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.