Agenda Item 11

Committee report

SPT

Cyber Resilience Framework update

Committee Audit and Standards

Date of meeting 28 August 2020 **Date of report** 11 August 2020

Report by Assistant Chief Executive

1. Object of report

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

2. Background

Cyber Resilience Framework

From an initial overview report presented to the Audit and Standards committee on 14 February 2020, members may recall, 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 (the Framework) with reporting deadlines therein.

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 has extracted 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 should 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

SPT position as at August 2020

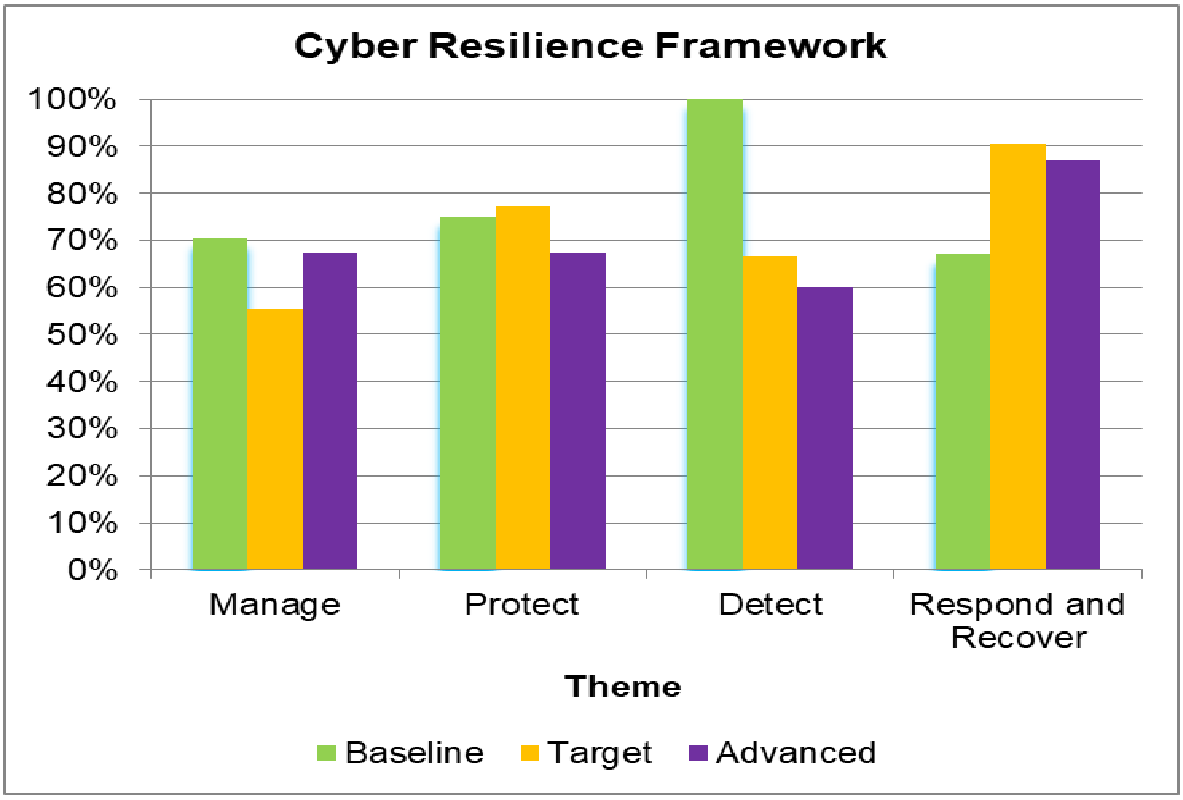
With reference to the above, officers have undertaken a systematic approach to complete the self-assessment which forms the Scottish Public Sector Cyber Resilience Framework.

In order to complete the self-assessment, input has been provided by Digital, Facilities, HR and Information Governance services and senior management.

The self-assessment has 434 questions in total. For each question a response has been recorded with associated evidence. Where a response is *'no'*, an action has been assigned to the question. Audit and Assurance assisted management to co-ordinate this initiative.

Cyber Resilience Framework graph

The following graph outlines SPT's position as at August 2020 for each of the four domains:



The collective summary percentages against each progression stage are as follows:

Baseline	73%
Target	75%
Advanced	70%
Overall	73%

Note: progression towards higher implementation rate of the Advanced stage may require additional resource allocation.

Management actions

From this initial self-assessment, an action log has been compiled for further management review. Each action will be evaluated and risk-assessed. The review process will assign a lead officer(s) and a timescale for completion.

In addition and to complement this workstream, the following management actions have been taken or are planned:

- 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;
- Internal training being developed for digital system administrators;
- Digital leadership training undertaken by the Assistant Chief Executive;
- Board level training to be delivered to members (date to be confirmed).

The letter from the Deputy First Minister and Cabinet Secretary for Education and Skills states that SPT is '*requested to report (annually) on progress on implementation of the Framework from July 2020 to 2021.'*

The prescribed reporting deadline has been met. The Audit and Standards committee will receive a Cyber Resilience Framework update in 2021.

4. Committee action

The committee is asked to:

i. note the contents of this report;

ii. note the position as at the date of this report on the Cyber Resilience Framework;

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