Committee report

# Digital assurance framework

**Committee** Audit and Standards

**Date of meeting** 30 November 2018 **Date of report** 7 November 2018

**Report by Assistant Chief Executive**

## 1. Object of report

To provide the committee with a report on the digital assurance framework within SPT from internal and external sources. This engagement is included in the Internal Audit plan for 2018/19.

## 2. Background

SPT makes extensive use of digital technology and networked systems. These systems support service delivery objectives, manage and pay suppliers and allow effective communication. Every part of SPT's business activities relies, in some way, on digital systems and technology.

Digital assurance framework

SPT seeks and receives digital assurance from internal and external sources.

Assurance mapping uses visual representation of assurance activities to demonstrate how they apply to a specific risk or set of compliance requirements.

The digital assurance map incorporates the following risk areas:

- the digital risks of the organisation;
- sub-sets of these risks (i.e. cyber resilience);
- compliance requirements (i.e. industry standards).

Assurance mapping takes the 'risk-set' or 'compliance-set' identified and details:

- the assurance provision for each of the risks or compliance requirements;
- the date of the most recent independent review on these assurances.

Assurance mapping identifies key areas of service delivery, internal and external assurance providers, and review dates.

The objective of this engagement was to assess and review internal and external assurance arrangements to assist in the compilation of the digital assurance map.

This engagement tested elements of the internal controls and mitigation against SPT 7: loss of digital infrastructure and SPT 22: governance arrangements.

## 3. Outline of findings

Digital assurance framework map

The digital assurance map, as at October 2018, can be found at Appendix 1.

Engagement testing (October 2018) identified a requirement to appoint a designated officer to co-ordinate the payment card industry data security standards (PCI DSS) accreditation. Engagement testing also identified a requirement to review performance management measures and the adequacy of pen testing arrangements.

There are some areas for improvement, and these areas have been addressed by three recommendations. Digital management have agreed to implement these recommendations, which are currently being actioned.

## 4. Conclusions

SPT seeks and receives digital assurance from internal and external sources. The digital assurance map outlines the key risk areas and mitigation, assurance provider(s) and the date of the last review.

The Audit and Assurance team has assisted in the development of the digital assurance map. Areas for improvement have been identified and three recommendations have been agreed.

Key controls exist and are applied consistently and effectively in the majority of areas tested in this engagement.

Reasonable assurance can be taken from the areas covered in this engagement.

## 5. Committee action

The committee is asked to note the contents of this report including the digital assurance map as at October 2018 and agree that the Audit and Assurance Manager submits a follow-up report on the implementation of the recommendations to a meeting in approximately six months.

## 6. Consequences

| | |
|---|---|
| Policy consequences | *None.* |
| Legal consequences | *None.* |
| Financial consequences | *None.* |
| Personnel consequences | *None.* |
| Social Inclusion consequences | *None.* |
| Risk consequences | *As detailed in the report and digital assurance map.* |

| | | | |
|---|---|---|---|
| **Name** | Valerie Davidson | **Name** | Gordon Maclennan |
| **Title** | **Assistant Chief Executive** | **Title** | **Chief Executive** |

For further information, please contact Iain McNicol, Audit and Assurance Manager on 0141 333 3195.

## Agreed action plan: Digital assurance framework

| No. | Recommendation | Priority | Action Proposed | Lead Officer | Due date |
|---|---|---|---|---|---|
| 1. | <u>Payment Card Industry Data Security Standard (PCI DSS)</u><br>Senior Management should appoint a designated officer to co-ordinate the PCI DSS certification process. Certifications and supporting documentation should be held centrally.<br>On completion of the certification process the co-ordinating officer should report any findings and actions required to the Strategy Group.<br>**Note:** the co-ordinating officer should ensure all staff with PCI DSS responsibilities are trained in their respective duties. | Medium | Digital management will co-ordinate the PCI DSS certification process. | Digital Manager | December 2018 |
| 2. | <u>Performance management</u><br><br>Digital management should regularly report changes/updates in digital assurance provision to senior management. | Medium | Digital assurance performance measures and reporting is subject to review/refresh. | Digital Manager | December 2018 |
| 3. | <u>Digital systems penetration (pen) testing</u><br><br>Digital management should risk assess the adequacy and frequency of digital systems pen testing. | Medium | External vendor pen testing will be reviewed in accordance with good practice guidelines. | Digital Manager | December 2018 |

**High**: A fundamental control that should be addressed as soon as possible;
**Medium**: An important control that should be addressed within three months;
**Low**: An issue which is not fundamental but should be addressed within six months to improve the overall control environment.