Agenda Item 8

Committee report

Contract audit of digital network security services

Committee	Audit and Standards		
Date of meeting	4 June 2021	**Date of report**	18 May 2021

Report by Assistant Chief Executive

1. Object of report

To advise the committee on the findings of a contract audit of digital network security services. This engagement was included in the annual Internal Audit plan for 2020/2021.

2. Background

SPT has a managed service for maintenance and support for its digital network services and telephony infrastructure.

This contract was awarded to Capita IT Services Limited for a period of three years following approval by the Partnership at its meeting of 14 December 2018.

The scope of the contract includes maintenance, service support, and testing of the digital network and infrastructure.

The objective of this engagement was to review and evaluate the contract monitoring arrangements in place for digital network security services.

This engagement tested elements of the internal controls and mitigation against SPT 7: loss of digital infrastructure, as identified in the Corporate Risk register.

3. Outline of findings

Engagement testing (March 2021) found that management arrangements were in place for this contract. As at the date of engagement testing, all payments made to the service provider were in accordance with the terms and conditions of the contract.

In addition, as identified during the audit testing, three variations have been made to this contract in relation to upgraded equipment to support digital service delivery.

The engagement identified a requirement to enhance contract performance management administration, and review the logical access controls to strengthen existing arrangements.

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

4. Conclusions

The Audit and Assurance team has undertaken a contract audit of digital network security services. Four recommendations have been agreed from this engagement.

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 internal controls in place.

5. Committee action

The committee is asked to note the contents of this report 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.*
Equalities consequences	*None.*
Risk consequences	*As detailed in the report.*

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

For further information, please contact Iain McNicol, Audit and Assurance Manager.

Reasonable assurance

Agreed action plan: Contract audit of digital network security services

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
1	Logical access The Network security (digital) service logical access controls and monitoring arrangements should be critically reviewed and refreshed. Access requirements and arrangements should be documented.	High	Network security (digital) service logical access controls and monitoring arrangements will be reviewed and where required refreshed. Technical and practical constraints will require to be considered, as part of the current retendering exercise. Access requirements and arrangements will be documented.	Digital Manager	June 2021
2	Procedures and Practices Network security (digital) service delivery outcomes should be documented together with any policy and procedural adherence requirements. Once documented, this guidance should be communicated to all relevant staff and service provider.	Medium	Network security (digital) service delivery outcomes and policy adherence requirements will be reviewed, documented and communicated to relevant staff and service provider.	Digital Manager	September 2021

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
3	Risk Assessment Network security (digital) service provision should be risk assessed regularly. This will help understand potential risks and vulnerabilities; conduct proper due diligence throughout the course of the contract and provide contingency arrangements and management of resources.	High	A retendering exercise for this contract is in progress. A risk assessment is part of this process.	Digital Manager	June 2021
4	Performance management Performance review meetings with the Network security (digital) service provider should be minuted and all actions should be logged and monitored. Digital management should periodically review the staff complement used by the contractor to service the contract. Digital Management should review performance monitoring and reporting to the stipulated contractual requirements and assurances provided by the service provider on service level agreements and service delivery outcomes.	Medium	Performance review meetings and actions will be logged and consolidated. Arrangements with the service provider will be reviewed /refreshed to include: • advising of changes to staff servicing the contract; and • alignment of performance monitoring and reporting arrangements with service delivery outcomes.	Digital Manager	September 2021

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.