Committee report

SPT

Regularity audit of digital change controls

Committee   Audit and Standards

Date of meeting 28 August 2020   **Date of report** 15 July 2020

Report by Assistant Chief Executive

1. Object of report

To advise the committee on the findings of a regularity audit of digital change controls. This engagement is included in the annual Internal Audit plan for 2020/2021.

2. Background

Every part of SPT's business activities relies, in some way, on digital systems and technology.

Digital change control is defined as:

'a systematic approach to managing all changes made to a product or system. Within information technology (IT), change control is a component of change management. The change control process is usually conducted as a sequence of steps proceeding from the submission of a change request.'

The objective of this engagement was to review and evaluate the digital change controls process.

This engagement tested elements of the internal controls and mitigation against SPT 6: Security and SPT 7: loss of digital infrastructure, as identified in the corporate risk register.

3. Outline of findings

Digital management have processes, procedures and practices in place for digital change control. However, the digital workflow procedure is not wholly reflective of current procedures and practices.

Engagement testing (June 2020) identified a requirement to review, enhance and strengthen the Digital change management process and procedures including Change Advisory Board membership and arrangements, workflow management and '*test'* environment administration.

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 regularity audit of digital change controls. Four recommendations have been agreed from this engagement.

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

Reasonable assurance can be taken from this engagement.

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

Title **Assistant Chief Executive**

Name Gordon Maclennan

Title **Chief Executive**

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

Agreed action plan: regularity audit of digital change controls

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
1	Digital change control process Digital management should review and strengthen the Digital change control process and procedures, including to: • meet enhanced digital security standards and practices; • risk assess stakeholder requirements; • review Change Advisory Board (CAB) arrangements and governance processes; • review supporting e-documentation; • enhance follow-up review procedures. Refresher training should be arranged for Digital staff and system administrators.	Medium	Digital management will review and enhance the current change control process in line with good practice guidance. Training will be provided to Digital team and system administrators on the change control process.	Digital Manager	October 2020
2	Change Advisory Board (CAB) Digital management should formalise arrangements and review the membership of the internal Change Advisory Board to include the following key stakeholders: • Digital service team; • Digital product lead officer(s); • Software engineer lead officer(s); • Systems owners/administrators, where required.	Medium	The membership of the CAB will be reviewed and revised to include Digital product team and systems administrators, where appropriate.	Digital Manager	October 2020

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
3	Testing of change controls administration Digital management should ensure that any change to systems, files and data is undertaken in a controlled manner. All significant changes should be only be actioned through the change control process, initially in a *'test'* environment, and subject to acceptance authorisation protocols before going *'live'*. Digital management should ensure that the change control log and e-stationery is reviewed and updated following testing, and • consider introducing a diary alert system to record follow up(s) and review; • review the process for requesting and authorising changes with external contractor(s)/product providers; • enhance monitoring reports to provide oversight of action (internal and external); • provide clear communications of decisions to all stakeholders. This should be a by-product of the Manage Engine Service Desk (Helpdesk system).	High	Where available, changes are initially processed in a *'test'* environment. The process for *'emergency'* changes will be reviewed. Change control testing, monitoring, log administration and review arrangements will be strengthened, where appropriate.	Digital Manager	August 2020
4	Separation of duties for Digital team Digital Management should ensure adequate separation of duties with regard to the change control process. Independent (secondary) approval should be required. **Note:** A risk based approach requires to be taken in relation to authorisation and governance for *'emergency'* changes with retrospective scrutiny protocol.	Medium	Digital management will review and enhance the current change control process including segregation of duties in line with good practice guidance.	Digital Manager	October 2020