Internal Audit Assurance

1. INTRODUCTION

1.1 The City of Edinburgh Council Internal Audit (IA) team performs one annual review to provide assurance over the controls established to mitigate specific key SEStran partnership risks.

1.2 The purpose of this paper is to provide an update on the outcomes of the 2022/23 SEStran IA review of the Thistle Assistance Programme, progress with completion of previously raised audit actions, and to request the Partnership's recommendations on potential areas for inclusion in the planned 2023/24 audit.

2. BACKGROUND, SCOPE, AND OUTCOMES OF 2022/23 IA REVIEW – THISTLE ASSISTANCE PROGRAMME

Audit Background

2.1 The Thistle Assistance programme aims to assist older people and those with disabilities or illness (protected characteristic) in using public transport. Stage one of the programme included development and operation of Thistle card and the mobile application, which advises the driver/conductor of passengers' protected characteristics and the assistance they need. Stage two involved creating awareness about the Thistle card/app symbols among transport operators, and stage three relates to the development of VoyagAR app, which aims to assist the passengers with protected characteristics in journey planning and way finding.

2.2 SEStran has engaged a third-party contractor to manage the generation and issuance of physical Thistle card. SEStran also administers generation and issuance of Thistle card for six other Regional Transport Partnerships (RTPs) and charges them production and marketing costs on a pro-rata basis.

2.3 The VoyagAR project has been awarded with a funding of £150k by Scottish Enterprise in 2019 and a further grant of £150k in 2020. The funding has been used to invite third party providers under the Innovate UK framework to initially deliver a proof of concept and subsequently deliver the final product (website and application). In addition to the cumulative awarded funding of £300k, SEStran has further internally funded this project with £37.5k for the contracted third-party supplier to deliver the final tranche of work by March 2023.

Audit Scope

2.4 The scope of the 2022/23 IA review was to assess the adequacy of design and operating effectiveness of the key controls supporting the effective implementation of Thistle Assistance programme. The review also followed up on the implementation of

management actions raised in the previously completed internal audit review of 'Active Travel Network Development'.

Audit Outcomes

2.5 The overall assessment of the review was 'some improvement required' (amber) and confirmed that the while some control weaknesses have been identified in the governance, risk and control frameworks supporting the Thistle Assistance programme, they provide reasonable assurance that risks are being managed and programme objectives should be achieved.

2.6 Areas for improvement identified in the review include:

i) formalising contracts and data sharing agreements with third party vendors, including regular review of their performance against key performance indicators (KPIs)

ii) reviewing software service provider's terms of agreement and cyber security controls to ensure continued operation of Thistle assistance mobile application

iii) developing a process to classify any business activity as a project and establishing formal project management governance arrangements.

2.7 Several areas of good practice were also identified as part of this review and are included in the opinion section of the detailed report.

2.8 Management has also addressed the low rated Internal Audit recommendations raised in the 2021/22 review of Active Travel Network Development by updating conflict of interest guidance and form in its Anti-bribery policy. The updated policy was presented for approval to March 2023 Performance and Audit Committee.

2.9 The full report is included at Appendix 1.

3. 2023/24 INTERNAL AUDIT REVIEW

3.1 The Council's 2023/24 Internal Audit annual plan will be presented to the Governance, Risk, and Best Value Committee on 14 March 2023, and includes one review for SEStran, which is consistent with the level of assurance provided in prior years.

3.2 The most significant areas of risk and potential areas for SEStran 2023/24 annual review will be discussed with the management team by July 2023, and the review is likely to be completed between September to December 2023.

4. RECOMMENDATIONS

The Board is requested to:

- note the progress with completion of an audit action raised in 2021/22 audit year

- note outcomes of the 2023/23 IA review of the Thistle Assistance Programme, and the associated costs, and

- provide insights or recommendations on key risks or areas of concern that the Board would like to recommend for inclusion in the 2023/24 IA review

Appendix 1: Internal Audit Report – Thistle Assistance Programme

Laura Calder
Head of Internal Audit, City of Edinburgh Council
E-mail: laura.calder@edinburgh.gov.uk | Tel: 0131 469 3077

Key contact:
Dheeraj Shekhar, Principal Audit Manager, City of Edinburgh Council
E-mail: dheeraj.shekhar@edinburgh.gov.uk | Tel: 0131 469 3221

Policy Implications	None
Financial Implications	SEStran is charged an annual fee for provision of the annual IA assurance review. The fee for 2022/23 is £5,000, which remains consistent with the 2021/22 fee applied.
Equalities Implications	None
Climate Change Implications	None

South East of Scotland Transport Partnership (SEStran)

Internal Audit Report

Thistle Assistance Programme

23 February 2023

OO2201

Overall Assessment	Some improvement required

Contents

Executive Summary

Overall opinion and summary of findings

Our review of the Thistle Assistance Project identified that while effective operational arrangements have been put in place to support the generation and issuance of Thistle cards, they are not formalised and supported by effective controls governance. Regular oversight is maintained on the third-party supplier contracted to develop the journey planning VoyagAR application, but this is not supported by formalised project management governance and controls.

Improvements in following areas have been identified to support effective governance of the Thistle Assistance project:

- formalised contracts and data sharing agreements with third party vendors and service providers, including key performance indicators (KPI) and service standards
- contract payments linked to service delivery and performance against KPIs
- review of the software service provider terms of agreement and cyber security controls to ensure continued operation of Thistle assistance mobile application
- clarity over classification of a business activity as project and establishing formal project management governance arrangements.

Areas of good practice

Our review identified:

- the card issuance process is fully documented
- the Thistle Assistance card was received within 14 days from application in our audit testing
- there are multiple ways to contact Thistle Assistance via phone, email and an online form
- recharging arrangements for Thistle card production and marketing costs are formally established with other Regional Transport Partnerships
- SEStran has a documented data protection privacy notice published on Thistle assistance website and Thistle app.

Audit Assessment

Audit Area	Control Design	Control Operation	Findings	Priority Rating
1. Thistle Assistance Card and Application Operations	🟠	🟠	Finding 1 – Thistle Assistance Card Finding 2 - Thistle App cyber security and data privacy controls	**Medium Priority**
2. Thistle Assistance Project Management	🟠	🟠	Finding 3 – VoyagAR Project Management	**Medium Priority**

Background and scope

See Appendix 1 for Control Assessment and Assurance Definitions

The Thistle Assistance programme aims to assist older people and those with disabilities or illness (protected characteristic) in using public transport. Stage one of the programme included development and operation of Thistle card and mobile application (app), which advises the driver/conductor of passengers' protected characteristics and the assistance they need. The app was further developed during the Covid-19 pandemic to advise drivers about passengers' face mask exemption, where applicable. Stage two involved creating awareness about Thistle card/app symbols among transport operators, and stage three relates to the development of VoyagAR app, which aims to assist passengers with protected characteristics in journey planning and way finding.

SEStran has engaged a third-party contractor to manage the generation and issuance of physical Thistle cards. SEStran also administers generation and issuance of Thistle cards for six other Regional Transport Partnerships (RTPs) and charges them production and marketing costs on a pro-rata basis.

The VoyagAR project was awarded funding of £150k by Scottish Enterprise in 2019 and a further grant of £150k in 2020. The funding has been used to invite third party providers under the Innovate UK framework to initially deliver a proof of concept and subsequently deliver the final product (website and application). In addition to the cumulative awarded funding of £300k, SEStran has further funded this project internally with £37.5k for the contracted third-party supplier to deliver the final tranche of work by March 2023.

Scope

The objective of this review was to assess the adequacy of design and operating effectiveness of the key controls supporting the effective implementation of Thistle Assistance programme.

The review also confirmed that the action raised in the previously completed internal audit review on 'Active Travel Network Development', to update the anti-bribery policy with a Conflict of Interest guidance and form, has been addressed. The updated policy is still in draft, but management has confirmed that it will be presented to the Performance and Audit committee in March 2023, along this audit report.

Risks

The review provides assurance in relation to the following SEStran corporate risks, relevant to the Thistle Assistance programme:

- R002 Financial risk
- R003 Project management risk
- R005 Third party service level agreements - Contract Management

Limitations of Scope

The following areas were excluded from scope:

- Technical elements of the Thistle assistance programme, including the accuracy of recharging arrangements to other partnerships

Reporting Date

Testing was undertaken between 10 January 2023 and 26 January 2023.

Our audit work concluded on 26 January 2023, and our findings and opinion are based on the conclusion of our work as at that date.

Findings and Management Action Plan

Finding 1 – Thistle Assistance Card

Finding Rating	Medium Priority

Audit testing of the Thistle card design and mail out process established that

- while the first invoice for card and leaflet design and printing is approved by the Partnership Director, there is no documented authorisation of designer/printer's appointment and commercial arrangement
- although the ongoing mail out of cards is performed by a printing vendor, the invoice is issued by a design agency
- there is not a formal agreement or contract between SEStran and the designer or mail-out printing supplier with established key performance indicators of service delivery. Management has confirmed that a formal contract is now being drafted
- there is no reconciliation performed between the order spreadsheet shared with the printer and the invoice paid
- a data sharing agreement has been drafted by the mail-out partner and shared with SEStran, but it has not yet been signed by both the parties.

Management have advised that they periodically perform mystery shopping *(secret shopping to gather information about service delivery and customer service quality)* of Thistle cards however, results of this activity are not formally recorded.

Customers can raise queries or complaints via telephone (voicemail), email or an online form. Management advised that they manage these queries/complaints using a shared email inbox, however, there is no log to record customer queries/complaints and monitor that they are addressed in a timely manner.

Risks

- **Contract Management** – Inability to manage contracts appropriately leading to potential service delivery risks
- **Financial –** Potential overbilling and duplicate payments in case of lack of reconciliation.
- **Reputational –** Customer queries and concerns are not addressed in a timely and appropriate manner

Recommendations and Management Action Plan: Thistle Assistance Card Controls

Ref.	Recommendation	Agreed Management Action	Action Owner	Contributors	Timeframe
1.1	Appointment of the leaflet designer and mail out printer should be formally authorised as per SEStran financial governance, and an agreement, with service delivery KPIs, should be formalised with all the third-party suppliers.	SEStran will formalise and put in place a new agreement with third party design and printing supplier.	Partnership Director	Programmes Manager	30/06/2023
1.2	SEStran should request confirmation details from the printer when a batch of card order sheet has been processed by the printer. A reconciliation among batch order sheet, batch confirmation sheet	Confirmation of batch processing and reconciliation to order sheet will be included in the new	Partnership Director	Programmes Manager	30/06/2023

	and invoice details should be performed before any payment is made to the printer.	agreement and process document, agreed with the printer, as part of ongoing process management.			
1.3	Data Exchange Agreement with the printer should be formalised and physically/digitally signed.	Data exchange agreement will be updated as part of new agreement with the third-party design and printing supplier.	Partnership Director	Programmes Manager	30/06/2023
1.4	Results of mystery shopping should be formally recorded and used as a tool for contract monitoring.	Mystery shopping results will be formally recorded and included in new process management flow and held in project folder.	Partnership Director	Programmes Manager	30/06/2023
1.5	A customer query/complaints log should be created and maintained to record details of received concerns with their resolution date and comments to monitor any thematic customer complaints, understand their concerns and ensure that they are addressed in a timely manner.	Customer query and complaints log will be formally recorded and included in the new process management flow and held in project folder.	Partnership Director	Programmes Manager	30/06/2023

Finding 2 – Thistle Assistance application cyber security and data privacy controls

Finding Rating	Medium Priority

The development and maintenance partner of SEStran's Thistle card mobile application (app) ceased to trade in 2022, and no alternative vendor had been appointed for app's maintenance and ongoing support, until 11 January 2023.

Internal Audit cannot comment on the effectiveness of mobile app's cyber security due to lack of available information. Our audit testing however found that while SEStran data privacy policy is linked on the application store, the Apple App store and Google Play Store are not populated with application specific data privacy information, resulting in a warning notice on both the store pages.

Risks

- **System and technology –** Service delivery would be affected if the application developed a software bug.
- **Reputational –** Potential customers may not download the app due to data privacy warning on the app stores

Recommendations and Management Action Plan: Thistle Assistance App cyber security and data privacy controls

Ref.	Recommendation	Agreed Management Action	Action Owner	Contributors	Timeframe
2.1	SLAs and the terms of agreement with new software services provider should be regularly monitored. Management should also consider exit clauses and strategies to be prepared for future contingencies, where the supplier ceases to operate.	New agreement is currently in place (Jan 2023) with a third-party software services provider and SLA monitoring has been put in place. Exit clauses will also be considered as part of SEStran risk management process for future contingency planning. SEStran will also be setting a new developer account on both the Apple and Google play store.	Partnership Director	Programmes Manager	SLA monitoring is ongoing. Risk register to be updated by 30/06/2023
2.2	SEStran should request and review assurance details from the new app developer on their cyber security controls, including data protection arrangements, on a periodic basis. Some examples of cyber security certifications and assurances include ISO 27001 standard, ISAE 3000/3402 assurance reports and Cyber Essentials certification.	Management will request the details of cyber security controls, including recommended assurance reports, from the new software services provider. These reports and details will be reviewed on an annual basis.	Partnership Director	Programmes Manager	30/06/2023
2.3	Data privacy information specifying how the app manages personal data should be uploaded to both Apple App store and Google Play store.	SEStran data management and information policy will be reviewed, updated and published on Apple and Android App stores.	Partnership Director	Programmes Manager	30/06/2023

Finding 3 – VoyagAR Project Management

Finding Rating	Medium Priority

Discussion with the team and management established that there is a lack of clarity in the team regarding identification of the development of VoyagAR app as a formal project managed by SEStran. The team have instead approached it as an outsourced activity supervised by SEStran through monthly meetings.

Consequently, there are no formally established project management arrangements including but not limited to the following best practice used in other SEStran projects:

- Project governance (Project Board and Senior Management reporting)
- Project progress/milestones review and monitoring
- Project risk management
- Project financial and budget management
- Project third party contract monitoring.

Risks

- **Project Management** – Potential under performance by outsourced contractor and failure to obtain best value delivery in the agreed timeframe.
- **Financial –** Lack of project governance leading to budgetary issues not being identified and addressed in a timely manner.
- **Governance –** Key person dependency risk and significant project delivery risks are not identified and escalated to Senior management / Committee members in a timely manner.

Recommendations and Management Action Plan: Project Governance

Ref.	Recommendation	Agreed Management Action	Action Owner	Contributors	Timeframe
3.1	Management should review the existing progress of the VoyagAR project and consider formalising project management controls, proportionately for the remainder of project.	Noted and agreed. Implementation of formalised project management controls will depend on successful completion and testing of final Voyager application in March 2023.	Partnership Director	Programmes Manager	30/06/2023
3.2	For all future projects, a Project Initiation Document should be drafted and agreed by the Project SRO and Senior Management, to formally establish a project with clearly defined project management arrangements.	SEStran will review the current arrangements and consequently implement the recommended actions, as needed.	Partnership Director	Business Manager/Programmes Manager	30/09/2023

Appendix 1 – Control Assessment and Assurance Definitions

Control Assessment Rating		Control Design Adequacy	Control Operation Effectiveness
Well managed	🟢	Well-structured design efficiently achieves fit-for purpose control objectives	Controls consistently applied and operating at optimum level of effectiveness.
Generally Satisfactory	🟢	Sound design achieves control objectives	Controls consistently applied
Some Improvement Opportunity	🟠	Design is generally sound, with some opportunity to introduce control improvements	Conformance generally sound, with some opportunity to enhance level of conformance
Major Improvement Opportunity	🔴	Design is not optimum and may put control objectives at risk	Non-conformance may put control objectives at risk
Control Not Tested	**N/A**	Not applicable for control design assessments	Control not tested, either due to ineffective design or due to design only audit

Overall Assurance Ratings	
Effective	The control environment and governance and risk management frameworks have been adequately designed and are operating effectively, providing assurance that risks are being effectively managed, and SEStran objectives should be achieved.
Some improvement required	Whilst some control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks, they provide reasonable assurance that risks are being managed, and SEStran objectives should be achieved.
Significant improvement required	Significant and / or numerous control weaknesses were identified, in the design and / or effectiveness of the control environment and / or governance and risk management frameworks. Consequently, only limited assurance can be provided that risks are being managed and that SEStran objectives should be achieved.
Inadequate	The design and / or operating effectiveness of the control environment and / or governance and risk management frameworks is inadequate, with several significant and systemic control weaknesses identified, resulting in substantial risk of operational failure and the strong likelihood that SEStran objectives will not be achieved.

Finding Priority Ratings	
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
Low Priority	An issue that results in a small impact to the achievement of objectives in the area audited.
Medium Priority	An issue that results in a moderate impact to the achievement of objectives in the area audited.
High Priority	An issue that results in a severe impact to the achievement of objectives in the area audited.
Critical Priority	An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency.