Partnership Board Meeting
Friday 22nd March 2019
Item A6(b). Internal Audit Plan

Internal Audit Plan

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 certain key SEStran partnership risks.

1.2 The purpose of this paper is to provide an update on the outcomes of the 2018/19 SEStran IA review; request the Partnership's insights on areas for potential inclusion in the scope of the planned 2019/20 review and request the Partnership's views regarding the requirement for an annual SEStran IA opinion.

2. SCOPE OF THE 2018/19 INTERNAL AUDIT REVIEW

2.1 The scope of the 2018/19 IA review assessed the design adequacy and operating effectiveness of the key controls established to ensure ongoing compliance with GDPR, with focus on SEStran's progress towards achieving the Scottish Government's Cyber Essentials Plus accreditation; and existing operational technology controls.

Review Outcomes

2.2 Our review confirmed that an adequate and appropriate control environment has been established to support SEStran's ongoing compliance with GDPR and ensure that the organisation is appropriately protected from cyber security.

2.3 Whilst some minor control weaknesses were identified, these are unlikely to have a significant impact on either GDPR compliance or security. Consequently, three Low rated findings were raised reflecting the opportunity to improve these controls.

2.4 The first finding reflects minor weaknesses in security arrangements supporting transfer of employee data to third party payroll and human resource providers that could be improved to ensure that personal sensitive employee information is appropriately protected.

2.5 The remaining findings highlight the need to improve employee awareness of cyber security and GDPR requirements through ongoing testing and ensure that all external assurance recommendations are documented and monitored to avoid potential key person dependency risks.

2.6 We also identified a number of areas of good practice applied by SEStran. These are included in the opinion section of the report (section 2).

2.8 The full terms of reference and final report are included at Appendices 1 and 2.

3. 2019/20 INTERNAL AUDIT REVIEW

3.1 The Internal Audit team has now completed their 2019/20 annual planning process, and the draft plan will be presented to the Council's Governance, Risk, and Best Value Committee for review and scrutiny on 19 March 2019.

3.2 The draft annual plan includes one 15-day Internal Audit review for SEStran. This is consistent with the level of assurance provided in prior years.

3.3 Initial discussions with SEStran management has highlighted the potential for IA to provide assurance in relation to the risks associated with development of the Regional Transport Strategy in 2019/20 review.

4. INTERNAL AUDIT ANNUAL OPINION

4.1 Public Sector Internal Audit Standards (PSIAS) require an organisation's Chief Internal Auditor to deliver an annual internal audit opinion that can be used by the organisation to inform its governance statement.

4.2 The annual internal audit opinion must conclude on the overall adequacy and effectiveness of the organisation's framework of governance, risk management and control.

4.3 The IA opinion would normally be based on the outcomes of a risk based IA plan designed to provide assurance across the full population of an organisation's risks, with focus on the most significant risks.

4.4 It should also be noted that IA is not the sole source of assurance provision for SEStran, as a number of additional external third line assurance providers are engaged (in addition to the annual external audit review of LPF's financial statements) to provide assurance across SEStran risks.

4.5 As IA delivers only one annual audit for SEStran that does not cover their entire population of risks, and is not their sole source of assurance provision, it is IA's view that it is not appropriate for IA to provide an annual opinion for SEStran.

4.6 It is IA's recommendation that the Committee and Board should instead place reliance on the collective outcomes of the annual IA review and assurance reviews completed by external assurance providers to form a holistic view on the effectiveness of the controls established by SEStran to manage their risks, and their governance arrangements.

5. RECOMMENDATIONS

5.1 The Board is requested to:

- note the outcomes of the 2018/19 IA review;
- confirm whether IA assurance in 2019/20 should focus on the adequacy and effectiveness of the framework supporting development of the

Regional Transport Strategy, and provide insights in relation to any other key SEStran risks and areas of concern that should be considered for inclusion in the 2019/20 IA review; and

- approve the IA recommendation that the Committee and Board should place reliance on the collective outcomes of the annual IA review and assurance reviews completed by external assurance providers, with no requirement for an annual IA opinion.

Lesley Newdall

Chief Internal Auditor, City of Edinburgh Council

E-mail: lesley.newdall@edinburgh.gov.uk | Tel: 0131 469 3216

March 2019

Appendix 1: Final Report

Appendix 2: Terms of Reference

Policy Implications	None
Financial Implications	SEStran is charged an annual fee for provision of the annual IA assurance review. The fee for 2017/18 was £5,000. The fee for 2018/19 is currently being quantified and will be discussed and agreed with management prior to finalisation.
Equalities Implications	None
Climate Change Implications	None

Appendix 1

The City of Edinburgh Council

Internal Audit

South East of Scotland Transport Partnership (SEStran)

Final Report

28 February 2019

OO1802

Contents

This internal audit review is conducted for the South East Scotland Transport Partnership under the auspices of the 2018/19 internal audit plan approved by the South East Scotland Transport Partnership Board in March 2018 The review is designed to help the South East Scotland Transport Partnership assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Although there are a number of specific recommendations included in this report to strengthen internal control, it is management's responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud. This is an essential part of the efficient management of the South East Scotland Transport Partnership. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings will be raised with senior management and elected members as appropriate.

1. Background and Scope

Background

The City of Edinburgh Council performs an annual Internal Audit review for the South East of Scotland Transport Partnership (SEStran). The scope of this review was directed by the SEStran management team and focuses on the organisation's most significant risks.

GDPR

The European Union (EU) General Data Protection Regulation (GDPR) became effective on 25 May 2018, and is designed to regulate the protection of natural persons in relation to processing their personal and personal sensitive data, and its free movement. It is expected that organisations will have established plans detailing the actions they need to implement to achieve compliance with the new regulations, with focus on addressing known legacy issues.

The legislation includes eight rights for individuals allowing easier access to their personal data held by organisations; a new fines regime; and a clear responsibility for organisations to obtain the consent of people they collect information on.

Consequently, it is essential that organisations have established appropriate data and records management frameworks that are aligned with GDPR requirements.

SEStran management has advised that advice was obtained from an information governance consultant who reviewed existing records management processes and developed training for team members. Additional legal advice was also obtained from Anderson Strathern.

Cyber Security

To ensure ongoing GDPR compliance, it is essential that organisations have established appropriate cyber security and operational technology controls to ensure that personal and personal sensitive data maintained in technology systems is appropriately secured.

In recent years, there has been a significant number of organisational data breaches including Facebook; Marriot Hotels; Morrisons; Uber; and local authorities. Many of these occurred due to weaknesses in external cybersecurity and internal operational technology controls designed to ensure that personal data held in systems is appropriately secured and protected.

The Scottish Government (SG) has noted that the importance of cyber resilience in Scotland's public bodies has never been greater, and has introduced the Public-Sector Action Plan for Cyber Resiliency (the Plan). The Plan sets out the key actions that the Scottish Government (SG), public bodies, and key partners were expected to take before the end of 2018 to further enhance cyber resilience across Scotland's public sector.

The SG has advised organisations to aim for either Cyber Essentials (essentially a self-assessment of their cyber controls), or Cyber Essentials Plus (CE Plus) accreditation, which involves completion of an independent assessment against the nine key actions included in the SG plan.

Management had advised that the majority of SEStran data is maintained in Microsoft Office 365, with archived data held on a server.

SEStran management had also advised that a cyber risk pre-assessment has been performed by an external consultant, resulting in the recommendation that SEStran should aim for cyber essentials plus accreditation, having already achieved Cyber Essentials certification. Accreditation for Cyber Essentials Plus was achieved 22nd February 2019.

Third party supplier management

To ensure ongoing compliance with GDPR requirements, it is important that organisations receive assurance from third parties (who process or store data on their behalf) confirming that they have established appropriate GDPR compliance frameworks; cyber security; and operational technology controls.

SEStran relies on a number of third parties for provision of outsourced services. Falkirk Council currently provide HR services; payroll is provided by the City of Edinburgh Council; technology services and support are outsourced to One Stop; and legal services are provided by Anderson Strathern.

SEStran payroll data is also provided to European organisations that provide funding.

Scope

The scope of this review assessed the design adequacy and operating effectiveness of the key controls established to ensure ongoing compliance with GDPR, with focus on progress towards CE Plus; existing operational technology controls; and third-party supplier management.

Our review was completed on 18th February 2019, and our findings and opinion are based on the outcomes of our testing as at that date.

2. Executive summary

Total number of findings: 3

Summary of findings raised	
Low	1. Third party supplier management.
Low	2. Staff knowledge and awareness of cyber security.
Low	3. External assurance recommendations.

Opinion

Our review confirmed that an adequate and appropriate control environment has been established to support SEStran's ongoing compliance with GDPR, and ensure that the organisation is appropriately protected from cyber security.

Whilst some minor control weaknesses were identified, these are unlikely to have a significant impact on either GDPR compliance or security. Consequently, three Low rated findings have been raised reflecting the opportunity to improve these controls.

The first finding reflects minor weaknesses in security arrangements supporting transfer of employee data to third party payroll and human resource providers that could be improved to ensure that personal sensitive employee information is appropriately protected.

The remaining findings highlight the need to improve employee awareness of cyber security and GDPR requirements through ongoing testing and ensure that all external assurance recommendations are documented and monitored to avoid potential key person dependency risks.

Our detailed findings and recommendations are laid out at Section 3 below.

Areas of good practice

The following areas of good practice were identified during our review:

- numerous policies such as Records Management; Data Protection; and Retention have been established to support ongoing compliance with applicable legislation and regulations;
- third parties are regularly engaged to provide external assurance provision (for example external reviews were commissioned to confirm the extent of GDPR compliance and the effectiveness of cyber security controls to support Cyber Essentials accreditation);
- Scottish Government Cyber Essentials certification and Cyber Essentials Plus Accreditation were achieved by February 2019;
- regular ongoing testing of technology systems to ensure effective and enhanced performance with minimal defects or issues;
- employees complete various training modules and refresher sessions, with key messages reinforced at team meetings, to further enhance awareness of policies;
- a breach register is maintained to record policy breaches and ensure that they are appropriately addressed; and
- a Register of Processing has now been drafted for immediate use.

3. Detailed findings

1. Third Party Supplier Management — Low

Contractually binding agreements exist between SEStran and their third party suppliers that outline the services that will be provided, and the information that will be processed. These are reviewed annually, with the agreement renewed where required.

At the time of our review, the contract for payroll service between SEStran and the City of Edinburgh Council (CEC) had been renewed, and the agreement with Falkirk Council for Human Resources support was being drafted.

Review of contracts and supporting service level agreements (SLAs) for both suppliers and the processes applied to manage employee data highlighted that:

- Supplier arrangements do not state requirements for secure transfer of employee payroll information (which includes personal sensitive employee information in relation to new starts; leavers; bank details; NI no; and salary details);
- Transfer of employee data is currently performed via secure external webmail for both Payroll and Human Resource services. Whilst occupational health documents attached in e mails are password protected, documents that include personal sensitive employee payroll data are not password protected;
- The contract and supporting SLA's for the City of Edinburgh Council has not yet been updated to specify how CEC will ensure that SEStran payroll data is transferred; managed; and processed in line with GDPR requirements. The agreement is due to be updated in May 2019 to include changes that affect processing; and
- There is no process documentation detailing how employee data is obtained; recorded and maintained on SEStran systems and transferred to Edinburgh and Falkirk Councils for processing as required by the new GDPR regulations at Article 30 (1) – (2).

  Management has advised that Advice was obtained from an external consultant who confirmed that SEStran is exempt from Article 30 due to their size.

Risk

- Personal sensitive employee data could potentially be compromised; and
- Potential breach of GDPR requirements.

Recommendation – City of Edinburgh Council contract review

The contract and supporting SLAs between SEStran and the City of Edinburgh Council should be updated to specify SEStran's expectations in relation to the secure transfer; management; and processing of employee payroll data in line with GDPR requirements.

Agreed Management Action

1. The SLAs will be updated to state how information will be secured and transferred; and
2. Password protection will be applied to all documents that contain personal sensitive employee data transferred between SEStran and third party suppliers with immediate effect, with passwords sent separately to the intended e mail recipient.

Owner: Jim Grieve, Interim Partnership Director **Contributors: Angela Chambers, Business Manager**	**Implementation Date: 31st May 2019**

Recommendation – employee data process mapping

The processes applied to obtain; record; maintain; and transfer personal sensitive employee data should be documented to meet new GDPR documentation requirements (Article 30 (1) – (2)).

Agreed Management Action

1. Advice was obtained from an external consultant who advised that SEStran is exempt from Article 30 due to their size; and
2. A register of processing will be developed and maintained detailing the nature of data received and how it is processed and managed by SEStran in line with Information Commissioner's Office guidance.

Owner: Jim Grieve, Interim Partnership Director **Contributors: Angela Chambers, Business Manager**	**Implementation Date: Complete**

2. Staff knowledge and awareness of Cyber Security and GDPR — Low

Employee updates on GDPR; Cyber Security; and other relevant areas are provided as and when required. Employees maintain individual training logs detailing the type of training undertaken and the date of completion. External training is also provided and employees attend where appropriate. Additionally, team meetings serve as a refresher session to cover relevant policies to ensure ongoing employee awareness and understanding.

Whilst comprehensive training and updates are provided for employees, these do not include knowledge testing.

Additionally, no phishing or cyber simulation exercises have been performed to assess ongoing employee awareness.

Risk

- Potential risk of breach of significant legislation (for example GDPR); and
- Significant technology impacts and potential GDPR breaches if SEStran suffers a cyber attack.

Recommendation -

SEStran should consider implementing training assessments in relation to significant legislative and regulatory requirements, and simulated cyber or phishing attacks to test employee awareness and confirm it is at an appropriate level.

Agreed Management Action

1. GDPR training now includes a video and a test at the end. Certificate of completion is received after successfully passing the test; and
2. The IT supplier has been engaged to arrange a phishing simulation exercise to test employee knowledge and awareness.

Owner: Jim Grieve, Interim Partnership Director **Contributors: Angela Chambers, Business Manager**	**Implementation Date: 31st May 2019**

3. External Assurance Recommendations

Low

SEStran engage with a number of external consultants to provide assurance in relation to compliance with applicable legislation and regulations, and effective management of risk.

The outcomes of these assurance reviews and implementation progress are not recorded and monitored to support update reporting to the Board. This results in key person dependency, as the Business Manager would have the task of ensuring that recommendations are actioned and included within reporting for Board Meetings to advise of changes.

Risk

- There is a key person dependency on the Business Manager to individually track and progress the actions;
- Oversight of the actions may be lost if not tracked;
- Unidentified issues may exist and go unaddressed.

Recommendation -

SEStran should design and implement a process to support ongoing monitoring external assurance recommendations to support effective management oversight and Board reporting, and reduce key person dependency risk.

Agreed Management Action

A tracker has now been developed and implemented to record all external assurance recommendations and their progress. The tracker includes sections for the type of assurance; the finding; recommendation; progress to date; and planned completion dates.

Owner: Jim Grieve, Interim Partnership Director **Contributors: Angela Chambers, Business Partner**	**Implementation Date: Complete**

Appendix 1 - Basis of our classifications

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on operational performance that would prevent SEStran from being able to operate in the long term*; or • ***Critical*** material monetary or financial statement impact in excess of external audit's financial statements materiality threshold that would impact SEStran's ability to continue as a going concern; or • ***Critical*** breach in laws and regulations that could result in material fines or long term consequences***;*** *or* • ***Critical*** impact on the reputation of the organisation which could threaten its future (long term) viability..
High	A finding that could have a: • ***Significant*** impact on operational performance that would prevent SEStran from being able to operate in the medium term**; or • ***Significant*** monetary or financial statement impact in line with external audit financial statements materiality threshold that requires and adjustment to the financial statements; • ***Significant*** breach in laws and regulations resulting in significant monetary fines and medium term consequences***;*** *or* • ***Significant*** impact on the SEStran's reputation that could threaten its future (medium term) viability.
Medium	A finding that could have a: • ***Moderate*** impact on operational performance that would prevent SEStran from being able to operate in the short term***; or • ***Moderate*** monetary or financial statement impact that is below the external audit financial statements materiality threshold, but requires an adjustment to the financial statements; or • ***Moderate*** breach in laws and regulations resulting in moderate fines and short term consequences; or • ***Moderate*** impact on the reputation of the organisation that could threaten its future (short term) viability.
Low	A finding that could have a: • ***Minor*** impact on operational performance that does not prevent SEStran from being able to operate; or • ***Minor*** monetary or financial statement impact that is below the external audit financial statements materiality threshold, and does not require an adjustment to the financial statements; or • ***Minor*** breach in laws and regulations with limited consequences; or • ***Minor*** impact on the reputation of the organisation that does not threaten its future viability.
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

* **Long term** – a period of one year or more

** **Medium term** – a period of 3 to 12 months

*** **Short term** – a period of 1 to 3 months

Terms of Reference – South East of Scotland Transport Partnership (SEStran)

To: Jim Grieve, Interim Partnership Director (SEStran)
Angela Chambers, Business Partner (SEStran)

From: Lesley Newdall, Chief Internal Auditor, City of Edinburgh Council

Date: 11th January 2019

The City of Edinburgh Council performs an annual Internal Audit review for the South East of Scotland Transport Partnership (SEStran). The scope of this review is directed by the SEStran management team and focuses on the organisation's most significant risks.

Background

GDPR

The European Union (EU) General Data Protection Regulation (GDPR) became effective on 25 May 2018, and is designed to regulate the protection of natural persons in relation to processing their personal and personal sensitive data, and its free movement. It is expected that organisations will have established plans detailing the actions they need to implement to achieve compliance with the new regulations, with focus on addressing known legacy issues.

The legislation includes eight rights for individuals allowing easier access to their personal data held by organisations; a new fines regime; and a clear responsibility for organisations to obtain the consent of people they collect information on.

Consequently, it is essential that organisations have established appropriate data and records management frameworks that are aligned with GDPR requirements.

SEStran management has advised that advice was obtained from an information governance consultant who reviewed existing records management processes and developed training for team members. Additional legal advice was also obtained from Anderson Strathern.

Cyber Security

To ensure ongoing GDPR compliance, it is essential that organisations have established appropriate cyber security and operational technology controls to ensure that personal and personal sensitive data maintained in technology systems is appropriately secured.

In recent years, there has been a significant number of organisational data breaches including Facebook; Marriot Hotels; Morrisons; Uber; and local authorities. Many of these occurred due to weaknesses in external cybersecurity and internal operational technology controls designed to ensure that personal data held in systems is appropriately secured and protected.

The Scottish Government (SG) has noted that the importance of cyber resilience in Scotland's public bodies has never been greater, and has introduced the Public-Sector Action Plan for Cyber Resiliency (the Plan). The Plan sets out the key actions that the Scottish Government (SG), public bodies, and key partners will be expected to take before the end of 2018 to further enhance cyber resilience across Scotland's public sector.

The SG has advised organisations to aim for either cyber essentials (essentially a self-assessment of their cyber controls), or cyber essentials plus (CE Plus) accreditation, which involves completion of an independent assessment against the nine key actions included in the SG plan.

Management has advised that the majority of SEStran data is maintained in Microsoft Office 365, with archived data held on a server.

SEStran management has advised that a cyber risk pre-assessment has been performed by an external consultant, resulting in the recommendation that SEStran should aim for cyber essentials plus accreditation.

Third party supplier management

To ensure ongoing compliance with GDPR requirements, it is important that organisations receive assurance from third parties (who process or store data on their behalf) confirming that they have established appropriate GDPR compliance frameworks; cyber security; and operational technology controls.

A range of services for SEStran are outsourced, such as: Falkirk Council currently provide HR services; Payroll function provided by CEC; technology services and support are outsourced to One Stop; legal services are provided by Anderson Strathern; and payroll data is also provided to European organisations that provide funding.

Scope

This review will assess the design adequacy and operating effectiveness of the key controls established to ensure ongoing compliance with GDPR, with focus on progress towards CE Plus; existing operational technology controls; and third-party supplier management.

Sample testing will be performed across the period 1st April 2018 to 31st March 2019.

Approach

Our audit approach is as follows:

- Obtain an understanding of the SEStran GDPR compliance framework; progress towards CE plus; operational technology controls; and supplier management;
- Identify the key risks associated with these processes;
- Evaluate the design of the controls in place to address the key risks;
- Test the operating effectiveness of the key controls on a sample basis; and
- Obtain evidence to confirm that previously raised Internal Audit recommendations have been effectively implemented and embedded.

The audit areas and related control objectives included in the review are:

Audit Area	Control Objectives
GDPR Compliance Framework	We will confirm: • That all recommendations resulting from the GDPR gap analysis have been effectively implemented; • That responsibility for GDPR and records management compliance and oversight responsibilities have been allocated at an appropriate level within the organisation; • That GDPR training has been provided to all existing employees and is included in induction training for all new employees; • That all operational processes (including all internal and external data flows) have been documented; • That a register of processing has been established detailing the nature of data processed and how it is protected; • Whether data privacy impact assessments (DPIAs) have been performed across all existing processes to ensure that data is appropriately protected, and that DPIAs will be performed for all new process and system changes; • That an appropriate and effective Subject Access Request (SAR) process has been implemented and is consistently applied; • That a process has been established to remove personal and private data from SEStran records upon request, or that the rationale for retaining the data can be provided; • That an appropriate and effective breach reporting process has been established; and • That management performs ongoing reviews to ensure that the records management policy is consistently applied.
Cyber Security and Operational Technology Controls	We will confirm: • That an appropriate plan has been established to support progress towards CE Plus accreditation; • That the plan includes implementation of the recommendations included in the independent cyber risk pre-assessment (notably resolution of the external website security risk); • That the organisation has established their key cyber security controls (including those provided by third parties), and regularly tests them (or receives assurance from third parties) that they continue to operate effectively; • That an independent assessor has been engaged to support CE Plus accreditation; • That training on cyber security and phishing has been provided to all employees; will be provided on an ongoing basis (to reflect increasing maturity and complexity of cyber threats) and is provided to all new employees as part of their induction training;

	• That a phishing or cyber simulation has been performed to assess levels of employee cyber awareness, and will be performed on an ongoing basis; • That personal and private data transferred to third parties is either transferred via securely encrypted e mail or a secure portal; • That all Microsoft 365 security controls have been configured and are consistently used (for example the requirement to set complex user passwords and change them on a regular basis); • That access to servers is appropriately secured with only limited access; and • That appropriate user management controls have been established with access to key systems appropriately allocated for new starts, and promptly removed for users.
Third Party Supplier Management	We will confirm: • That appropriate GDPR and technology security requirements have been established in all third-party contracts; and • That regular ongoing assurance is obtained from third parties regarding the effectiveness of their ongoing GDPR and cyber and technology security controls.
Identification of Risks	Confirm that risks associated with ongoing GDPR compliance; cyber and technology security controls; and transfer of data to and processing by third parties are regularly assessed and reflected in the organisation's risk register.
Implementation of IA recommendations	Obtain evidence to confirm that the recommendations raised in the 2017/18 SEStran Governance Internal Audit Governance review have been effectively implemented and sustained.

Internal Audit Team

Name	Role	Contact Details
Lesley Newdall	Chief Internal Auditor	0131 469 3216
Saima Afzal	Internal Auditor	0131 469 3082

Key Contacts

Name	Title	Role	Contact Details
Jim Grieve	Interim Partnership Director, South East of Scotland Transport Partnership	Key Contact	0131 524 5160
Angela Chambers	Business Manager, South East of Scotland Transport Partnership	Key Contact	0131 524 5154

Timetable

Fieldwork Start	15th January 2019
Fieldwork Completed	29th January 2019
Draft report to Auditee	5th February 2019
Response from Auditee	15th February 2019
Final Report to Auditee	25th February 2019

Appendix 1: Information Request

It would be helpful to have the following available prior to our audit or at the latest our first day of field work:

- Access to systems and databases relevant to obtain evidence of third party suppliers;
- Copy of the relevant policies for Cyber Security, Information Security and third party supplier management.

This list is not intended to be exhaustive; we may require additional information during the audit which we will bring to your attention at the earliest opportunity.

Appendix 2: Roles and Responsibilities

City of Edinburgh Council Internal Audit

The role of Internal Audit is to act as an independent, objective assurance and consulting function, designed to add value and improve the operational effectiveness of the organisation. Internal Audit has unrestricted access to all activities undertaken in the organisation to independently review and report on the governance, risk management and control processes established by management.

Auditors will ensure they conduct their work with due professional care and in line with the requirements of the Public Sector Internal Audit Standards and other relevant professional standards.

The responsibilities of Internal Audit in respect of individual audit assignments are detailed in Appendix 3.

South East of Scotland Transport Partnership

It is Management's responsibility to develop and maintain sound systems of risk management, internal control, and governance and for the prevention and detection of irregularities and fraud. Internal Audit work should not be seen as a substitute for Management's responsibilities for the design and operation of these systems.

Management will co-operate with Internal Audit on assignments and provide access to records, systems and staff as required within a reasonable timeframe following the request.

Where an audit report is delivered, management are required to provide formal responses to all recommendations, including specifying responsibility and anticipated dates for the implementation of the solutions within two weeks of the draft report being issued. They are also responsible for the implementation of the solutions and this implementation will be monitored and subject to follow-up review.

Internal Audit work is performed solely for the South East of Scotland Transport Partnership (SEStran) and solely for the purposes outlined above. Reports and documents prepared by Internal Audit should not be provided to anyone else.

The responsibilities of the auditee in respect of individual audit assignments are detailed in Appendix 3.

Appendix 3: Audit Process

Area	Principles	Further guidance
Planning the audit	Agreeing the audit scope and objectives	• Internal Audit will determine and make arrangements for sufficient resources to achieve the agreed audit engagement objectives. This will be based on an evaluation of the nature and complexity of each engagement, time constraints and available resources. • An initial planning meeting will be held between Internal Audit and SEStran management. The planning meeting will be held in advance of the audit fieldwork commencing. The purpose of the meeting will be to agree the scope and objectives for the review, requirements during the audit and a reporting and closeout timetable. • SEStran management will identify the employees who have the relevant knowledge and are best placed to answer questions in relation to the audit scope. Management will be responsible for notifying these staff of the audit scope and any other requirements agreed with Internal Audit during the planning meeting. • Internal Audit will be responsible for organising meetings with relevant staff.
Audit fieldwork and planning	Timely communication of issues identified during fieldwork	• The Auditee will be informed of the progress of the audit on a regular basis. • Any issues identified during the fieldwork by Internal Audit will be discussed with the relevant staff to ensure that they are accurate and proposed recommendations are valid and achievable. • Any material issues (Critical) will be raised by Internal Audit with the Partnership Director and Business Partner immediately as they arise.
Reporting	Closeout meeting to discuss and agree the internal audit report	• The closeout meeting will be undertaken with the Partnership Director and Business Manager within 2 weeks of the audit fieldwork being completed. • Internal Audit will provide management with a copy of the draft report within 2 weeks of completing the fieldwork.

Area	Principles	Further guidance
Reporting	Management response to internal audit report	• The Auditee will have 2 weeks to provide management comments. During this period, where appropriate, the Auditee should consult with management team on the findings and recommendations in the Internal Audit report. • Internal Audit will issue the final report within 1 week of receipt of management comments to the Partnership Director.
Reporting	Reporting of internal audit findings to the [enter name of appropriate scrutiny committee] Committee	• Internal Audit will present the audit report annually to the SEStran Performance and Audit Committee. The update report will summarise the findings arising from the finalised internal audit report. It will also include progress on implementation of prior year internal audit recommendations.
Follow up	Monitoring the implementation of internal audit recommendations	• A questionnaire will be issued to be completed by the Auditee to allow opportunity to comment directly to the Chief Internal Auditor on the satisfaction of the audit service provided. This forms part of the Internal Audit Quality Review program. • Internal audit will track the status of all open recommendations. Recommendations that are overdue will be reported to the SEStran Performance and Audit Committee on an annual basis. Internal Audit will advise management of all open recommendations and invite them to provide evidence that the recommendations have been actioned.