Risk Management Framework

1. INTRODUCTION

1.1 This paper provides the Committee with a first full draft version of the proposed risk register, which is an integral part of SEStran's Risk Management Framework.

1.2 The report also highlights to the Committee an update on a specific risk to the Partnership: Cyber Security.

2. BACKGROUND

2.1 Performance and Audit Committee has received six-monthly updates of the risk register in recent years, as part of SEStran's commitment to a framework of risk management within the organisation. This will continue and a copy of the new condensed Risk Register is attached for discussion and further comment. SEStran has been using a Risk Register to record, report and evaluate risks within the organisation since May 2008 and the Committee should be assured that all risks are reviewed regularly by the relevant staff. The Committee is invited to discuss the identified risks included in the new format and whether there is need for further amendment or addition.

3. CURRENT KEY RISKS

3.1 Under the Digital/IT entry on the risk register, the report highlights the ongoing actions/lobbying of Scottish Government's (SG) Cyber Security Public Sector Action Plan. As reported in September, we have raised our comments with the Scottish Government on the Action Plan and have since welcomed their revisions to timescales and funding, allowing public bodies a full year to implement a cyber essentials pre-assessment and key action list. However, we have highlighted that, whilst the outcome of the pre-assessment is unknown at present, a further extension may be required to successfully achieve Cyber Essentials certification.

3.2 SEStran has also stated its concern that there is no provision from SG for further financial support being available to assist with implementation (should this be required), particularly for small public bodies like most RTPs. The Government's response is that if a public body finds that the costs of any remediation work are very high, they should contact SG to discuss. SG highlighted in their initial response to SEStran that if they found that lots of public bodies were unable to meet the controls without very high expenditure, they might look at whether any economies of scale could be achieved. Therefore, the Partnership effectively has a full year to put in place these basic controls, which we anticipate will be sufficient time to do so, and to take account of this requirement within budgets. It is a key risk to our security of information and records, but also a financial

risk to the Partnership, pending the outcome and cost of implementation of actions identified from the assessments.

3.3 The Committee should note that a meeting has been scheduled with our IT provider, Onestop, to discuss cyber resilience and cyber essentials accreditation; seeking their opinion on the appropriate level of accreditation suitable for SEStran. A verbal update will be given at the meeting and progress will be reported to future meetings.

3.4 SEStran's Business Continuity Management Plan, which sets out the procedures to be followed in the event of loss of normal operations, is an integral part of its cyber security framework. The plan is usually reviewed in September, however, given the significance of the SG's Action Plan, SEStran is seeking to postpone this exercise until January to allow adequate time to consider the implications of implementation.

4. RECOMMENDATIONS

4.1 The Committee is requested to discuss and comment upon the latest version of the Risk Register, and:

4.2 asked to note the update on key identified risk under Digital/IT of Cyber Security Assessments;

4.3 asked to note that discussions will be progressed to determine the appropriate level of Cyber Essentials accreditation required and further updates will be brought to future meetings;

4.4 asked to agree to the Business Continuity Management Plan review being postponed until January 2018.

Angela Chambers
Business Manager
November 2016

Appendix 1: SEStran Risk Register

Policy Implications	Potential revision to disaster recovery procedures.
Financial Implications	Potential cost of implementation of Cyber Security assessments.
Equalities Implications	None
Climate Change Implications	None

Appendix 1

Risk Detail	Risk Category	Gross Risk Assessment						Planned Response/Mitigation	Net Risk Assessment						Risk After Mitigation	Date and Owner
		Probability		Impact		Risk Score			Probability		Impact		Risk Score			
Policy Appraisal: Poor Quality Lack of consultation	Strategic	1	Remote	3	Moderate	3	Low Risk	*Partnership Director regularly horizon scanning for new relevant policies and responds accordingly using delegated powers if a response is required. New policy forums also enable greater visibility and integration of local policies into regional strategy*	1	Remote	2	Minor	2	Low Risk	Low. Partnership staff also continue to monitor their networks for relevant policy discussions. Director chairs the reelvant SCOTS Transportation Working Group.	November 2017 Partnership Director
Project Appraisal and Delivery: Incomplete or of poor quality Late Delivery	Reputational	2	Unlikely	4	Major	8	Medium Risk	*Monthly monitoring and management intervention by the project officer, and over-seen by the Head of Programme. Key regional projects such as RTPI has regular communication with key cilents and service providers, including standing quarterly stakeholder meetings.*	2	Unlikely	3	Moderate	6	Low Risk	*Low. Regular monitoring and management/project team meetings gave all across the organisation a clear view of progress and timescales greatly reducing risk*	November 2017 Head of Programmes
Digital/IT: Server failure Comms failure: phones Website	People	3	Possible	4	Major	12	Medium Risk	*SEStran has an up-to-date Management Plan for Business Continuity, clearly available in the office and remotely. Wesbite has a maintenence contract as does RTPI system, which regular updates and patches to avoid failure.*	3	Possible	2	Minor	6	Low Risk	*Low. We have employed IT consultants to deliver our IT and phone. Our website contract includes updates as part of a quarterly mainteance contract.*	November 2017 Business Manager
Reputation: Social Media hacked and inapproriate comments Lack of brand awareness	Reputational	3	Possible	3	Moderate	9	Medium Risk	*Social media passwords are high security; focussed brand enhancement work is undertaken, project as regularly monitored via monthly meetings*	3	Possible	2	Minor	6	Low Risk	*Low. Passwords are securely stored, updates of software regularly undertaken by staff and server providers. Work in ongoing to deliver a new brand for the Partnership as agreed at September 2017 Board meeting. PArtnership staff continue to promote and advocate our policies via speaking, writing or wider networking*	November 2017 Partnership Director
Statutory Duties: Fail to comply with statutory duties and legallly challenged e.g. Transport 2005 Act; Community Empowerment Act 2015; Equality 2010 Act; Public Services Reform 2010 Act; new Gender Balance Bill. Freedom of Information and REcords Management Impact on accounts and statement of governance	Legal and Regulatory	1	Remote	4	Major	4	Low Risk	*Monthly monitoring and management intervention by the project officer, and over-seen by the Partnership Director. We have a published Equality Outcomes and Records Management Plan. We have partipcation request information on the website etc*	1	Remote	2	Minor	2	Low Risk	*Low. Regular monitoring and programming of our statutory duties is undertaken by the Partnership Director, Head of Porgrammes and Business Manager. Including attednance at relevant training and guidance sessions identified by statutory partners. We also*	November 2017 Partnership Director

Appendix 1

Financial: Significant deviation from budgeted spend	Financial	1	Remote	3	Moderate	3	Low Risk	*Budget and spend monitored by CEC Accountants, in dialogue with SEStran. CEC reports to Performance and Audit Committee & Board, quarterly. Necessary interventions by Director.*	1	Remote	2	Minor	2	Low Risk	***Low**. There is also a current consultation on the ability for RTPs to carry forward expenditure to seek to*	November 2017 Partnership Director
a) Pay awards: Each 1% uplift in pay provision equates to an increase of £3,300.	Financial	4	Probable	1	Insignificant	4	Low Risk	*Alignment with Scottish Local Government pay policy*	4	Probable	1	Insignificant	4	Low Risk	***Tolerate***	November 2017 Partnership Director
b) Staff recharges - EU projects: There is a risk that opportunities for additional funding through income for EU projects may reduce.	Financial	5	Highly Probable	3	Moderate	15	High Risk	*Any shortfall in emloyees cost recharges will be offset by a corresponding reduction in Projects Budget expenditure.*	4	Probable	2	Minor	8	Medium Risk	***Medium**: Other funding sources will be pursued*	November 2017 Partnership Director
c) Inflation: There is a risk that there is an increase in price inflation.	Financial	5	Highly Probable	1	Insignificant	5	Low Risk	*Allowance will be made for specific price inflation and budgets adjsuted in line with current cost forecasts.*	5	Highly Probable	1	Insignificant	5	Low Risk	***Tolerate***	November 2017 Partnership Director
d) Delays in payment of external grants results in additional short-term borrowing costs.	Financial	3	Possible	2	Minor	6	Low Risk	*SEStran grant claims for projects are submitted in compliance with grant funding requirementsto ensure minimal delay in payment. Ongoing monitoring of cash flow will be undertaken to manage exposure to additional short-term borrowing costs.*	3	Possible	1	Insignificant	3	Low Risk	***Low:** Accruals procedure in place, along with financial planning.*	November 2017 Partnership Director
e) Sources of additional income to the Partnership may become constrained in the current economic climate and/or due to changes in operating arrangements.	Financial	4	Probable	3	Moderate	12	Medium Risk	*Develop revenue budget to take account of most likely level of external income in 2018/19.*	4	Probable	3	Moderate	12	Medium Risk	***Tolerate:** Adapt expenditure accordingly*	November 2017 Partnership Director
f) Funding reductions: Reduction in funding from Scottish Government and/or council requisitions	Financial	3	Possible	4	Major	12	Medium Risk	*Subject to decision by the Partnership Board, the draft budget will be prepared based on a 5% reduction in funding from council requisitions and Scottish Government grant. Continue to source and develop external funding.*	3	Possible	4	Major	12	Medium Risk	***Tolerate:** Manage organisation in accorance with available funding but ability of organisation to deliver RTS objectives will inevitably be reduced.*	November 2017 Partnership Director
HR: Pension Liabilities Redundancy Contingency Inappropiate Behaviour Staffing/Incapacity	People	1	Remote	3	Moderate	3	Low Risk	*HR policies and procedures have a regular review cycle, policy training and code of conduct are given to all members at indcution, staffing levels and workload are monitored by senior management on a monthly basis. We have lobbied UK and Scottish Government on Redundancy Modification Orders. Managers hold regular meetings and formal reviews with staff. Engage with Pension Fund as required.*	1	Remote	2	Minor	2	Low Risk	*The risk is low. We have access to direct advice from Falkrrk Council. Have undertaken a recent pay and grading review and update relevant policies.*	November 2017 Partnership Director

Appendix 1

Corporate: Removal of RTPs as part of the review of the National Transport Strategy.	Strategic	4	Probable	3	Moderate	12	Medium Risk	*Regular monitoring being developed, lobbying for funding, inputs to NTS2 and STPR. Partnership Director is engaged in the NTS2 review, co-chairing one of the 4 strategic working groups and co-ordinating SCOTS responses to the review. The Partnership Chair represents all RTPs on the NTS2 Review Board and has sought and received assurances around retention of functions and undertakings transfer from Scottish Ministers.*	4	Probable	2	Minor	8	Medium Risk	*Medium risk. The NTS2 review set up a review of Roles and Responsbilities group. Transport Scotland have appointed consultants to support this governance review and will report in Spring 2017. There is also risks associated with the Planning and Enterprise + Skills reviews for RTPs. These cannot be reduced at present, however we are engaged fully and lobbying for the best interests of the Partnership.*	November 2017 Partnership Director
EU Exit: Impact on learning and funding	Financial	5	Highly Probable	4	Major	20	High Risk	*The Partnership has sought to engage in as many reelvant EU projects and funds as it can whilst UK authorities are allowed to access these funds. This should mitigate the short-term impact of any EU Exit negotitated and implemented in the short-term.*	5	Highly Probable	4	Major	20	High Risk	*The risk is still High as there is significant uncertainty around the medium (3-5year) horizon for access to funds. However, in the current time, we have sought to mitigate by getting as much access to funds and projects as possible in the short-term and seek to monitor and tolerate the ongoing risk this poses to a key revenue and knowledge streams for the PArtnership.*	November 2017 Head of Programmes

Likelihood		Severity		Risk Score		At Risk
1	Remote	1	Insignificant	1	Low Risk	System and Technology
2	Unlikely	2	Minor	2		Reputational
3	Possible	3	Moderate	3		Strategic
4	Probable	4	Major	4		Financial
5	Highly Probable	5	Catastrophic	5		Governance
				6		Specific Operational
				8	Medium Risk	External
				9		Legal and Regulatory
				10		People
				12		Physical
				15	High Risk	
				16		
				20		
				25		

Impact				
Descriptor	**Score**	**Health and Safety Impact**	**Impact on Service and Reputation**	**Financial Impact**
Insignificant	1	No injury or no apparent injury.	No impact on service or reputation. Complaint unlikely, litigation risk remote.	Loss/costs up to £5000.
Minor	2	Minor injury (First Aid on Site)	Slight impact on service and/or reputation. Complaint possible. Litigation possible.	Loss/costs between £5000 and £50,000.
Moderate	3	Reportable injury	Some service distruption. Potential for adverse publicity, avoidable with careful handling. Complaint expected. Litigation probable.	Loss/costs between £50,000 and £500,000
Major	4	Major injury (reportable) or permanent incapacity	Service disrupted. Adverse publicity not avoidable (local media). Complaint expected. Litigation expected.	Loss/costs between £500,000 and
Catastrophic	5	Death	Service interrupted for significant time. Adverse publicity not avoidable (national media interest.) Major litigation expected. Resignation of senior management/directors.	Theft/loss over £5,000,000

Likelihood		
Descriptor	Score	Example
Remote	1	May only occur in exeptional circumstances.
Unlikely	2	Expected to occur in a few circumstances.
Possible	3	Expected to occur in some circumstances.
Probable	4	Expected to occur in many circumstances.
Highly Probable	5	Expected to occur frequently and in most circumstances.

Impact					
Catastrophic	5	10	15	20	25
Major	4	8	12	16	20
Moderate	3	6	9	12	15
Minor	2	4	6	8	10
Insignificant	1	2	3	4	5
Likelihood	Remote	Unlikely	Possible	Probable	Highly Probable

Maintain existing measures in place.
Review control measures. Even if the risk is low, there may be things that can be done to bring the risk rating down to minimal.
Improve control measures. If the Rating Action Band is greater than 3 or 4 then a review of the exisiting safety/control measures needs to be done, where
Improve control measures immediately and consider stopping work activity until risk is reduced.