RISK MANAGEMENT FRAMEWORK POLICY

DOCUMENT VERSION CONTROL

Date	Author	Version	Status	Reason for Change
Oct 2021	SEStran	1.0	DRAFT	Policy Drafted
Nov 2021	SEStran	1.1	FINAL	Approved by Performance & Audit Committee

Introduction

This document sets out SEStran's approach to risk management and outlines the key objectives, strategies, and responsibilities for the management of risk across the organisation. It applies to all SEStran staff and should be applied consistently across the organisation.

The management of risk is integral to SEStran's governance arrangements and the outputs from effective risk management include assurance, compliance and enhanced decision making.

What is Risk Management?

Risk and Risk Management are defined as follows:

Risk is defined as:

"the threat that an event or action will adversely affect an organisations ability to achieve its objectives and to successfully execute its strategies"

Risk Management *is defined as:*

"the process by which risks are identified, evaluated, controlled and monitored."

Risk Management Policy

SEStran is committed to the management of risks within its control to safeguard employees, protect assets, preserve or enhance service delivery, maintain effective stewardship of public funds and promote a favourable corporate image.

However, risk management is about being risk aware and making the most of opportunities rather than avoiding risk altogether. To meet our objectives, it is appreciated that some risks must be taken. It is important, however, that these risks are actively controlled.

SEStran's risk management aims and objectives are as follows:

- to initiate measures which will reduce SEStran's exposure to risk and potential loss;
- to establish standards and principles for the efficient management of risk;
- seek to identify, assess, control and report on any risk that will undermine the delivery of SEStran's priorities, at a strategic and operational level;
- promote awareness of risk and embed the approach to its management throughout the organisation.
- to provide a component of effective corporate governance and management practice;
- provide a sound basis for integrating risk management into decision making;

- when managing and controlling risks, actions will be proportionate - the cost and time of our efforts should be in balance with the potential impact and likelihood of the risk.

Responsibilities

The SEStran **Partnership Board** through its **Performance and Audit Committee** has responsibility for the risk management arrangements of the organisation.

The **Partnership Director** has overall responsibility for risk management for SEStran.

The **Management Team** has day to day responsibility for the systems of internal control, including consideration and application of risk management.

Employees are encouraged to make suggestions that assist and contribute to risk control measures.

Internal/External Audit provide independent assurance on the effectiveness of control measures in place.

Risk Registers

Risks are recorded on a risk register, either the corporate risk register or project risk register.

Risks are categorised into ten risk areas, namely: strategic, financial, legal and regulatory, people, system and technology, reputational, governance, external, specific operational and new project income. The risk register format includes the following information:

- Risk number
- Risk detail
- Gross risk assessment score
- Planned response/mitigation
- Net risk assessment score
- Risk after mitigation
- Date and owner
- Target risk tolerance level

Risks are regularly reviewed by the Management Team and a risk report is presented to the Performance and Audit Committee twice a year. This report is included in the Partnership Board agenda for noting.

Risk Management Process

The risk management process is broken down into the following steps:

Risk Identification

Risk identification is an ongoing activity, with individual risks and the impact and/or likelihood of risk regularly changing. The process of risk identification supports SEStran to determine what outcomes/objectives it is looking to achieve and identify any threats and/or opportunities to aid achievement.

There are several sources that help with risk identification, for example: business planning; compliance and assurance activities; partnership meetings; management/team meetings; project meetings; working groups; analysis of recurring complaints/feedback; horizon scanning; new/changing legislation.

A table outlining risk descriptions and impacts which can be used to assist in identifying areas of risk can be found at **Appendix 1**

Risk Analysis

Once a risk is identified the risk is assessed. Risks are assessed considering the ***likelihood*** of the risk occurring and if that risk was to occur, what the ***impact*** (i.e. consequences) on the organisation would be.

Likelihood is categorised on a scale of 1 to 5 with one being remote and five being highly probable. Impact will also be assessed on a scale of 1 to 5 with one being insignificant and 5 being catastrophic. Likelihood and impact are multiplied together to obtain a total gross risk score as illustrated in the table below:

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

A table setting out the risk impacts descriptions, classified by three event types: health and safety; service and reputation and financial can be found at **Appendix 2**

A table setting out the risk likelihood descriptions can be found at **Appendix 3**

Risk Management

Once risks have been identified and assessed they must be managed and controlled, applying the following guidance:

Risk Appetite

Risk appetite is defined as the amount and type of risk that an organisation is willing to take to meet their strategic objectives and deliver services.

The risk register format steers risk owners into considering risk appetite when updating a risk entry. Consideration must be given to the risk score before and after existing mitigating action and the final tolerable risk target status.

SEStran's risk appetite is summarised below:

Risk Rating	Net Risk Assessment	Risk Appetite Response
High	15-25	Unacceptable level of risk exposure which requires action to be taken urgently.
Medium	7-14	Acceptable level of risk but one which requires action and active monitoring to ensure risk exposure is reduced
Low	1-6	Acceptable level of risk based on the operation of normal controls. In some cases, it may be acceptable for no mitigating action to be taken.

Risk Response

There are four categories of risk response:

Terminate: risk avoidance – where the proposed activity is out with the current risk appetite level;

Treat: risk reduction – where proactive action is taken to reduce the likelihood or impact of an event occurring or limiting the consequences should it occur (e.g. install virus protection software on all computers)

Transfer: risk transfer – where the liability for the consequences is transferred to an external organisation in full or part (e.g. insurance cover)

Tolerate: where certain risks are accepted

Risk Mitigation

Risk mitigation are the controls and actions put into place to reduce the likelihood of the risk occurring or minimise the impact of the risk if it does occur. Mitigation can be taken from various sources of assurance, including:

- assurances from management designed controls that are being implemented on a day to day basis, including the framework of policies, procedures, processes and controls in place (system of internal controls);
- assurances from the risk management arrangements and compliance functions, including oversight functions (e.g. health and safety) within SEStran that co-ordinate, facilitate and provide assurance over the risk and control environment;
- assurance from Internal Audit, which carries out an annual review to provide independent assurance over the controls established to mitigate certain key risks.

SEStran also receives assurance from external bodies, including external auditors.

The residual risk which remains after taking account of the relevant mitigations is the net risk. A target risk score, which is the tolerable level of risk that SEStran is aiming for, is applied to each net risk. The target risk scores are set out at **Appendix 4.**

Risk Monitoring and Reporting

Circumstances and business priorities can, and do, change and therefore risks, opportunities and their circumstances need to be regularly reviewed. This review should include the following questions:

- Are the risks still relevant?
- What progress has been made in managing the risk?
- Given the progress made, do the risk scores need revising?
- Are any further actions needed? If so, then what should these be?

Risk should be a regular item on the agenda for management team meetings and it is the responsibility of the risk owner to review risks on a regular basis.

SEStran's risk management framework is supported through agreed reporting and assurance arrangements. The arrangements include:

- The Partnership Board through the Performance and Audit Committee reviews and approves risk management policies and strategies;
- The Performance and Audit Committee will;
    - receive bi-annual Risk Management reports to review the risk register;
    - considers an annual report from Internal Audit
- The management team maintains, reviews and updates the SEStran Risk Register on the key risks facing the organisation on a regular basis
- Risks associated with projects will be maintained, reviewed and updated by the responsible manager/officer.

Appendix 1: Risk Description and Impacts Table

Ref	Type of Risk	Description	Impact
R001	Strategic	Inability to design and / or implement a strategic plan or strategy for SEStran.	Lack of clarity regarding future direction and structure of SEStran impacting quality and alignment of strategic decisions
R002	Financial	Inability to perform financial planning; deliver an annual balanced budget; manage cash flows; and confirm ongoing adequacy of reserves	SEStran is unable to continue to deliver in line with strategic objectives; inability to meet financial targets; adverse external audit opinion; adverse reputational consequences
R003	Reputational	Adverse publicity because of decisions taken and / or inappropriate provision of sensitive strategic, commercial and / or operational information to external parties	Significant adverse impact to SEStran's reputation in the public domain
R004	Governance	Inability of management and members to effectively manage and scrutinise performance, and take appropriate strategic, financial and operational decisions	Poor performance is not identified, and decisions are not aligned with strategic direction
R005	External	Inability to effectively manage SEStran's most significant supplier and partnership relationships	Inability to deliver strategy and major projects within budget and achieve best value
R006	Legal / regulatory	Delivery of services and decisions are not aligned with applicable legal and regulatory requirements	Regulatory censure and penalties; legal claims; financial consequences
R007	Specific Operational	Inability to deliver projects and programmes effectively, on time and within budget	Inability to deliver projects; achieve service improvements; and deliver savings targets
R008	System and technology	Potential failure of cyber defences; network security; application security; and physical security and operational arrangements	Inability to use systems to support services; loss of data and information; regulatory and legislative breaches; and reputational consequences
R009	People	Employees and / or citizens suffer unnecessary injury and / or harm	Legal; financial; and reputational consequences
R010	New Project Income	Inability to attract new projects to fill the funding gap left by diminishing EU projects/Brexit	Inadequate funding streams and lack of innovation.

Appendix 2: Risk Impact Descriptions

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 disruptions. 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 £5,000,000.
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

Appendix 3: Risk Likelihood Description

Likelihood		
Descriptor	Score	Example
Remote	1	May only occur in exceptional 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.

Appendix 4: Risk Appetite Target Score Range

Risk Description	From	To	Commentary
Strategic	Low	Medium	SEStran has a low to medium appetite in relation to its strategic risks and aims to ensure effective delivery of its commitments in line with agreed timescales. Strategic delivery is monitored through ongoing reporting processes and governance processes.
Financial	Low	Medium	SEStran has a low to medium appetite in relation to financial risk and may be prepared to accept some risk, subject to: • setting and achieving an annual balanced revenue budget, in line with legislative requirements • maintaining an unallocated general reserve fund, in line with legislative requirements Financial risk is set out in SEStran's Governance Scheme.
Reputational	Low	Medium	SEStran is prepared to tolerate a low to medium level of occasional isolated reputational damage. Media response protocols are set out in the Governance Scheme.
System and Technology	Low	Medium	SEStran has a low to medium appetite in relation to system and technology risk. The risk appetite will vary depending on the nature, significance and criticality of systems used, and the services they support. Risks are managed through ongoing use of inbuilt technology, security controls, encryption, data loss prevention, firewalls and vulnerability scanning, plus a range of security protocols and procedures. SEStran has achieved Cyber Essentials Plus accreditation.
Governance	Low	Low	SEStran has a low appetite in relation to governance and decision making. The partnership's governance arrangements are detailed in the Governance Scheme. No officer or member may knowingly take or recommend decisions or actions which breach legislation.

Specific Operational	Low	Medium	SEStran has a low to medium appetite in relation to specific operational risks. The Partnership Director and Management Team are expected to design, implement and maintain appropriate programme, project management and governance controls to manage these risks.
External (Suppliers/contractors/ partnerships)	Low	Medium	SEStran has a low to medium appetite in relation to external risks. The appetite will vary depending on the criticality of the service or third-party support. SEStran has an established procurement process, supported by the Contract Standing Orders and use of Public Contract Scotland frameworks.
Legal and Regulatory	Low	Low	SEStran aims to fully comply with all applicable regulatory and legislative requirements. No officer or member may knowingly take or recommend decisions or actions which breach the law.
People	Low	Low	SEStran recognises that accidents can occur because of unknown and/or unplanned events and has an appetite to fully comply with all relevant health and safety requirements to minimise any health and safety risks that could potentially result in loss of life or injury.
New Project Income	Medium	High	SEStran has a medium to high appetite in relation to attracting new projects to enable innovation and attract new funding streams. SEStran has an established procurement process, supported by the Contract Standing Orders and use of Public Contract Scotland frameworks. Financial risk is set out in SEStran's Governance Scheme.