SPSO Risk Management Handbook

Version	*Description*	*Date*	*Author*
0.1	Approved by Senior Management Team and AAC	2014 Jul	Senior Personal Assistant
1.0	Published on SPSO website	2015 Apr	Senior Personal Assistant
1.1	Audited	2016 Nov	Internal Auditor
2.0	Published on SPSO website	2016 Dec	Corporate Services Manager
3.0	Published on SPSO website	2017 May	Corporate Services Manager
4.0	Approved by Leadership Team	2018 Aug	Ombudsman
5.0	Approved by Leadership Team	2019 Sep	Corporate Services Manager
6.0	Approved by Leadership Team	2020 Nov	Corporate Services Manager
7.0	Approved by Leadership Team	2023 Jul	Corporate Services Manager

Note: Highlighter is used in this document to indicate outstanding actions or where links to other documents under review, are required.

Contents

Risk Management and Incident Reporting Policy

Scope

1. This policy sets out the steps that need to be followed in order to identify and manage business risk. It also outlines procedures to support staff to navigate the system of incident reporting, incident investigation and associated learning.

Key Points

2. Risk management is part of: business planning, strategic and operational decision making, and business continuity.

3. In order to manage risk effectively, the SPSO needs to define their risk appetite; to ensure resources are prioritised in the right areas and to encourage management to take appropriate risks where it will generate the highest value.

4. A risk needs to threaten the achievement of the SPSO's strategic and business aims to be included in the risk register.

5. One of the key elements of internal control will be ensuring that the Leadership Team (LT) give appropriate consideration to risk when making decisions.

6. With a constantly changing business environment and evolving priorities, the risks the SPSO faces change over time and need to be reviewed regularly.

7. The risk register should only contain risks that the SPSO is in a position to manage and control or to minimise the impact on the SPSO should the risks materialise.

8. The LT should ensure that risk assessment is embedded into the corporate and performance management, business planning and financial reporting processes and not carried out as an isolated exercise.

9. It is recognised good practice to record and report data, security, and health and safety incidents which occur to ensure that learning and improvement takes place.

Background

10. This policy outlines the steps that need to be followed in order to identify and manage key risks to the achievement of the SPSO's business objectives in line with Best Practice. Risk management should therefore be closely linked to the business planning process. There should also be a link between risk management, business planning and plans for business continuity.

11. Risks arise from possible threats to the SPSO's ability to achieve its objectives, and failure to take advantage of opportunities. Risk can be either external (for example, changes in economic or political circumstances or the actions of organisations with which the SPSO has close links) or internal (for example, failure of systems or the actions of staff). Managers must remain continually watchful for new or developing risks.

12. Additionally, should a data, security, or health and safety incident occur, this document outlines the procedures for incident reporting, incident investigation and associated learning.

Risk Management

Risk Registers

13. The Strategic and Operational Risks will be set at the start of each year, as part of the business planning process which involves all staff.

14. All staff will be notified of the annual Risk registers once approved by the LT. In-year updates and amendments will be disseminated by LT members as appropriate to their teams.

15. The strategic and operational risk registers are the mechanism by which the links are made between strategic aims and operational delivery and performance of services.

Strategic risk register

16. The strategic risk register sets out the strategic risks that impact on several areas of business and relate specifically to the Strategic Plan.

17. The plan for the year will be signed off by the LT, taking into account advice from the AAB.

18. The risk register will identify both Strategic risks and Operational risks.

19. It is reviewed and updated quarterly, or ad hoc if needed. Changes must be agreed by the LT and recorded on the appropriate update tab.

Operational risk register

20. The Operational Risk register sets out the risk, and its management, in relation to delivery of the annual business plan. It will be reviewed and updated quarterly by the LT. Suggestions for inclusion and updates may be submitted by staff in two ways:

20.1. through the quarterly operational performance meetings, reporting changes to the LT representative; and
20.2. as required in response to specific amendments identified through risk assessments of proposals to LT, or approval of items at LT meetings.

21. See also the section on Embedding the Process.

Roles and Responsibilities

22. Annex 1 sets out the roles and responsibilities and the timetable for managing risk in SPSO. Through a process of corporate evaluation of the known risks, the LT should aim to arrive at an overall list (grouped as appropriate) of the key risks confronting the SPSO. This list will incorporate those key risks facing teams, as identified by team managers during their regular operational meetings with their senior manager, which threaten achievement of the SPSO's strategic and business objectives.

23. As part of their responsibility for internal control and as part of an effective business planning process the LT should meet at least quarterly to review the key business risks associated with achievement of the SPSO's strategic objectives. It is for the LT to judge the impact of all potential key risks (not only financial risks) and to consider how they should be managed.

24. The five main objectives of the quarterly review of the risk register should be to:

24.1. discuss, evaluate and agree the list of key business risks which might affect the ability to deliver departmental objectives and targets;
24.2. assess existing controls (the measures in place to reduce or limit risk);
24.3. determine the appropriate response to each risk;
24.4. allocate responsibility for managing each risk, and
24.5. agree future review procedures.

Risk Appetite

25. The SPSO recognises that assessing the level of principal risks it accepts will inform the planning and decision-making the organisation undertakes to achieve its aims of delivering beneficial outcomes to its stakeholders. The aim is to balance the methods we use to manage the principal risks in line with the risk appetite so we can both support innovation and the imaginative use of resources and continue to provide a best value public service.

26. The SPSO will seek to control all probable risks which have the potential to:

26.1. cause significant harm to service users, staff, visitors and other stakeholders;
26.2. compromise severely the reputation of the organisation;
26.3. have financial consequences that could endanger the organisation’s viability;

26.4. jeopardise significantly the organisation's ability to carry out its core purpose; and

26.5. threaten the organisation's compliance with law and regulation.

27. Descriptors used to describe our risk appetite across the different functions include:

27.1. AVOID: No appetite. Not prepared to accept any risks.

27.2. AVERSE: Prepared to accept only the very lowest levels of risk, with the preference being for ultra-safe delivery options, while recognising that these will have little or no potential for reward / return.

27.3. CAUTIOUS: Willing to accept some low risks, while maintaining an overall preference for safe delivery options despite the probability of these having mostly restricted potential for reward / return.

27.4. MODERATE: Tending always towards exposure to only modest levels of risk in order to achieve acceptable, but possibly unambitious outcomes.

27.5. OPEN: Prepared to consider all delivery options and select those with the highest probability of productive outcomes, even when there are elevated levels of associated risk.

27.6. HUNGRY: Eager to seek original/creative/pioneering delivery options and to accept the associated substantial risk levels in order to secure successful outcomes and meaningful reward / return.

28. Risk appetite statements helps SPSO establish a threshold of impacts we are willing and able to absorb in pursuit of our strategic objectives.

Risk Evaluation

29. Taking each of the risks in turn the LT will discuss and rate the inherent likelihood of each risk occurring, and its impact on quality, cost and timescales should it occur. This is done by assessing and awarding a numerical value where the lowest risk =1 and the highest risk =5. These rating values are then combined to provide an overall inherent risk rating using the following scale:

21-25 = Critical	unacceptable level of risk exposure that requires immediate mitigating actions
12-20 = High	unacceptable level of risk which requires controls to be put in place to reduce exposure

5-10 = Medium acceptable level of risk exposure subject to regular active monitoring

1-4 = Low acceptable level of risk subject to regular passive monitoring

30. The control actions currently in place for each risk are detailed and the risk is re-assessed with a current score. The overall significance of the risk is then rated as low, medium, high or critical.

Response to Risk

31. Once the key risks have been identified and assessed, the LT consider how to manage them to complete this aspect of internal control. Consideration is given to new risks resulting from changed business objectives.

32. Response to risk can be to:

32.1. tolerate it - because there is no cost effective control and the risk can be adequately monitored;
32.2. transfer it - to another party, for example, by contracting out;
32.3. terminate it - by closing down the activity; or
32.4. treat it - by taking appropriate action to manage the risk through the introduction of appropriate controls.

33. The response in any particular case will depend on the nature and impact of the risk and the extent to which the risk can be managed. Where appropriate, the action required to manage the risk is then described, and the key manager(s) responsible for implementing the action detailed. This action will be mirrored in the Business Plan.

Risk Toleration Level

34. The response to each risk will determine the amount of risk the LT is prepared to accept before action (or further action) is deemed necessary to manage the risk. The framework is designed to encourage the identification and management of key risks through a systematic approach. Consideration is given to the business tolerance for the risk and a target score for each risk is agreed. Any further planned controls to mitigate the risk and reach the target score are recorded. These actions will be mirrored in the current business plan.

Ownership of Risk

35. The LT will seek to promote a management environment in which all staff participate in the identification, notification and management of business risks. Risk management should be embedded throughout the SPSO at all appropriate levels.

Controls

36. Controls relate to procedures that help to ensure management objectives and policies are carried out. They ensure that risks, which may inhibit the achievement of objectives, are kept to a minimum. Controls include measures, which can range from approval and authorisation procedures to performance reviews, to segregation of duties.

37. Controls fall into four categories and can be defined as follows:

Directive	designed to ensure that a particular outcome is achieved
Preventive	designed to limit the possibility of an undesirable outcome being realised
Detective	designed to identify occasions when undesirable outcomes are realised
Corrective	designed to correct undesirable outcomes, which have been realised

38. One of the key elements of internal control will be ensuring that the LT have adequate advice on risk when reaching policy decisions.

39. Controls should be proportional to the risk. For the most part, they should, for example, be designed to give a reasonable assurance of confining likely loss to the toleration levels agreed by the LT. Control actions have associated costs and it is important that they offer value for money in relation to the risks being controlled and are mainly designed to contain risk rather than obviate it.

Review and Assurance

40. The AAB scrutinise and provide the SPSO with advice about its risk management. This includes considering management responses to the work of internal Auditors, particularly in relation to the effectiveness of the SPSO's internal control systems. This is achieved through a programme of internal audits in line with the LT's internal audit programme and reporting to the AAB and LT.

Embedding the Process

41. The LT will ensure that risk assessment is embedded into the corporate and performance management, business planning and financial reporting processes. The LT's approach to internal control is based on the underlying principle of line management's accountability for risk management and internal control. The risk

register supports the assurances given by/ to the Ombudsman as Accountable Officer in relation to the signing of the annual governance statement.

42. The LT and AAB follow an agreed timetable for formal review of the risk register, and other sources of assurance, whilst bearing in mind that the key risks faced by the SPSO may change and that the adequacy of the internal control system requires regular re-assessment.

43. The 'top down' approach to risk management in the SPSO acknowledges that day-to-day control rests with the LT and SPSO managers. However, in order to fully embed risk management, risk assessment and the impact on risk registers should be prepared with staff involvement.

44. All decisions taken that have an impact on the way business is delivered and on strategic management of the organisation, and issues that emerge through the year should include a risk assessment. The use of the meetings cover sheet is normally sufficient for this purpose, but when considering the impact of issues, new areas of work or individual projects, the LT may commission a more in-depth risk assessment/ interrogation.

45. Risk assessment must make specific reference to risks in the operational risk register, and if applicable to the strategic risk register. The impact of risk must set out clearly

    45.1. Is there an existing applicable risk in the operational risk register?

    45.2. If yes, will the policy/ procedure/ action proposed maintain, mitigate, control or increase the likelihood or impact of specific, referenced, existing risks? If so a recommendation should made for changes to the risk register.

    45.3. If no, is this a new risk? If so a recommendation should be made either about adding a new risk, either permanently or temporarily, or conducting a more in-depth risk analysis.

46. It is the LT sponsor's responsibility to ensure that the risk assessment on cover sheets is sufficiently robust and detailed. Papers presented with insufficient risk assessment are likely to be deferred so the risk assessment can be carried out.

Assurance for the Leadership Team

47. The sources of assurance that the LT use are:

    47.1. LT and AAB review of the risk management process;
    47.2. review of the risk register;
    47.3. performance and risk indicators;

47.4. risk assessment in relation to decision-making;
47.5. views of line management and key staff;
47.6. independent monitoring activities, and
47.7. audit.

Annex 1: Roles and Responsibilities in Managing Risk

Responsibility	*Role*
AAB	To advise on the management of risk by the SPSO and give assurance about the adequacy of the internal control systems
External and Internal Auditors	To give preliminary consideration to the key corporate risks facing the SPSO and provide advice to the AAB, Accountable Officer and LT
Ombudsman as Accountable Officer	To ensure that the risks which the organisation faces are dealt with in an appropriate manner in accordance with relevant aspects of best practice in corporate governance
LT as Risk Owners	To ensure that the organisation manages strategic and operational risk effectively through the development of a risk management process
Director, Corporate Services Manager and Internal Auditors	To support the LT in the effective development, implementation and review of the risk register
Managers	To manage risk effectively in their particular areas, including where appropriate, maintaining risk registers
All Staff	To manage risk effectively in their jobs and to contribute as necessary to the risk register process

Annex 2: Timetable for the Management of Risk by the Leadership and Management Teams

Timing	*Action*
March	LT review strategic risks as part of the business planning process.
Throughout Year	The LT review the risk register on an ongoing basis when decision-making and quarterly. The LT present to the AAB for comment and advice. Internal Auditors review risk management process using the four elements of the Audit Scotland risk management tool kit and provide a report to the AAB. This will be spit over two years and reviewed in detail as follows: • the work in year one will focus on commitment, leadership, responsibility, accountability and planning; with the focus being the management at a strategic level. • year two, the focus will be on resources, sharing information and best practice, performance, financial and staff management. With the focus being on the doing and implementation. External Auditors audit risk management process as part of their annual audit for Audit Scotland.
Twice Yearly (minimum)	AAB review and give advice and assurance about risk management.

Back to the main Contents page