SPSO Risk Management and Incident Reporting 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
8.0	Approved by Leadership Team	2025 Jan	Corporate Services Manager
9.0	Approved by Leadership Team	2026 Apr	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 overview

Scope

1. This policy outlines the steps to identify and manage key risks to the achievement of the SPSO's business objectives. Additionally, should a data, security, or health and safety incident occur, this document outlines the procedures for incident reporting, incident investigation and associated learning.

2. Risk Management is the combined activities required to identify, understand and control exposure to uncertain events which may threaten the achievement of objectives.

3. Incidents are those events that have already occurred and which have an effect on the achievement of objectives. Issues are certain or ongoing circumstances which will have, or are already having, an effect upon the achievement of objectives. The SPSO record and report data, security, and health and safety incidents which occur to ensure that learning and improvement takes place.

4. 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.

Risk management

Key points

1. Risk management is an integral part of the business planning cycle, strategic and operational decision making, and ensuring business continuity. One of the key elements of internal control is ensuring that the Leadership Team (LT) give appropriate consideration to risk when making decisions.

2. 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 remain continually watchful for new or developing risks.

3. The SPSO has defined our risk appetite across the different business areas; to ensure resources are prioritised in the right areas and, if appropriate, to take some risks where it will generate the highest value. With a constantly changing business environment and evolving priorities, the risks the SPSO faces change over time and, therefore, are reviewed regularly.

4. A risk needs to threaten the achievement of the SPSO's strategic and business aims to be included in the risk register. The risk register only contains risks that the SPSO is in a position to manage and control, or to minimise the impact on the SPSO should the risks materialise.

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

Risk registers

6. The Strategic and Operational Risks will be set at the start of each business year, as part of the business planning process which involves all staff. The annual Strategic Risk Register is published alongside the annual Business Plan.

7. In-year updates and amendments are published quarterly, and disseminated by LT members to their teams where appropriate.

8. 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.

9. Risks are defined in if/then/resulting statements, with a nominated risk owner who is also accountable for the achievement of the corresponding business plan objectives.

Strategic risk register

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

11. The plan for the year is signed off by the LT, taking into account advice from the AAB, and published.

12. It is reviewed and updated quarterly, or ad hoc if needed. In-year changes are agreed by the LT are recorded in a summary table. The updated register is published.

Operational risk register

13. The Operational Risk register sets out the risk, and its management, in relation to delivery of the annual business plan, and is aligned with each business area's annual plan. It is reviewed and updated quarterly by the team manager and associated LT representative. Suggestions for inclusion and updates may be submitted by staff in two ways:

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

14. See also the section on Embedding the Process.

Roles and responsibilities

15. The annex 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.

16. As part of their responsibility for internal control and as part of an effective business planning process the LT 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.

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

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

Risk appetite

18. 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.

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

19.1. cause significant harm to service users, staff, visitors and other stakeholders;
19.2. compromise severely the reputation of the organisation;
19.3. have financial consequences that could endanger the organisation's viability;
19.4. jeopardise significantly the organisation's ability to carry out its core purpose; and
19.5. threaten the organisation's compliance with law and regulation.

20. Descriptors used to describe our risk appetite across the different business areas include:

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

20.2. 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.

20.3. 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.

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

20.5. 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.

20.6. 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.

21. 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

22. The framework is designed to encourage the identification and management of key risks through a systematic approach. Risks are evaluated at three levels: inherent, current, and tolerance level.

Inherent level:

23. 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

Current level:

24. The control actions currently in place for each risk are detailed and the effect these actions have on the inherent evaluation of the risk is considered. The risk is re-assessed with a current score. The overall significance of the risk is then rated as low, medium, high or critical.

25. 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 also given to new risks resulting from any new or changed business objectives.

26. Response to risk can be to:

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

27. 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.

28. 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.

Toleration level

29. Consideration is given to the business tolerance for the risk and a target score for each risk is agreed, in proportion to the risk appetite, organisation size and current resources. This will determine the amount of risk the LT is prepared to accept before action (or further action) is deemed necessary to manage the risk.

30. 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

31. The LT promote a management environment in which all staff participate in the identification, notification and management of business risks. Risk management is embedded throughout the SPSO at all appropriate levels.

32. The Risk Owner, who is responsible for the achievement of the corresponding business plan objectives, is accountable for:

32.1. deploying and directing the resources needed to achieve the objective,
32.2. tracking performance and implementing any improvement actions,
32.3. monitoring the risks throughout each risk's lifetime,
32.4. reporting on the status of the risks,
32.5. ensuring appropriate risk controls are put in place, and
32.6. ensuring the risk management policy is followed.

Controls

33. 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.

34. 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

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

36. 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.

37. 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.

Embedding the process

38. The LT 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.

39. 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.

40. 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.

41. 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.

42. 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

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

    42.2. 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.

    42.3. 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.

43. 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.

Review and assurance

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

    44.1. LT and AAB review of the risk management process;
    44.2. review of the risk register;
    44.3. performance and risk indicators;
    44.4. risk assessment in relation to decision-making;
    44.5. views of line management and key staff;
    44.6. independent monitoring activities, and
    44.7. audit.

45. 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.

Annex: roles, responsibilities and timetable 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, twice yearly.
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. Internal Auditors review risk management process and provide a report to the AAB. External Auditors audit the risk management process as part of their annual audit for Audit Scotland.
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. Quarter four LT review strategic risks for the new business year, as part of the business planning process. Throughout the year, the LT review the risk register on an ongoing basis when decision-making and quarterly for reporting purposes.
Corporate Services Manager	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

Back to the main Contents page

Incident reporting

1. The purpose of reporting incidents is to ensure that learning and improvements are made that may prevent similar incidents from occurring in the future.

Immediate management of incidents

2. The member of staff who discovers or is informed of a high risk incident, if not a manager, is responsible for informing a manager immediately. The manager will take immediate necessary action to ensure the safety of those involved. The manager is responsible for assessing the situation and taking appropriate immediate action to:

    2.1. ensure the wellbeing and safety of all those involved;
    2.2. manage the incident and minimise potential adverse effects of the incident, and
    2.3. minimise the risk of the incident occurring again in the future.

Reporting incidents

3. The manager is responsible for ensuring that the incident is fully recorded on the Specific Incident Log [template] and stored in the appropriate Incident Log folder with any documentation relating to the incident. The completion of the Specific Incident Log must be within ten working days of the incident. This log will record:

    3.1. the significant action, decision or event
    3.2. mitigating actions taken, noting the dates and time, and
    3.3. any follow-up action required.

4. There is additional guidance in the Information Governance handbook for data security incidents, which must be reported immediately to the CIGO or DPO, as these incidents may potentially be reported to the ICO within 72 hours.

5. The Head of Corporate and Shared Services (or, in their absence, another member of the LT) should be informed as soon as possible of the incident and the action being taken. Once the incident is closed and the log has been completed, the manager should forward a link to the LT, including recommendations to update the operational risk register.

6. All incidents where there is any suspicion of fraud, bribery, corruption or a similar offence must be reported to the Ombudsman immediately. The Ombudsman will notify the Chair of the AAB. In the Ombudsman's absence or if the matter concerns the Ombudsman it should be reported immediately, in confidence, to the Chair of the AAB.

Back to the main Contents Page