

# SPSO Risk Management

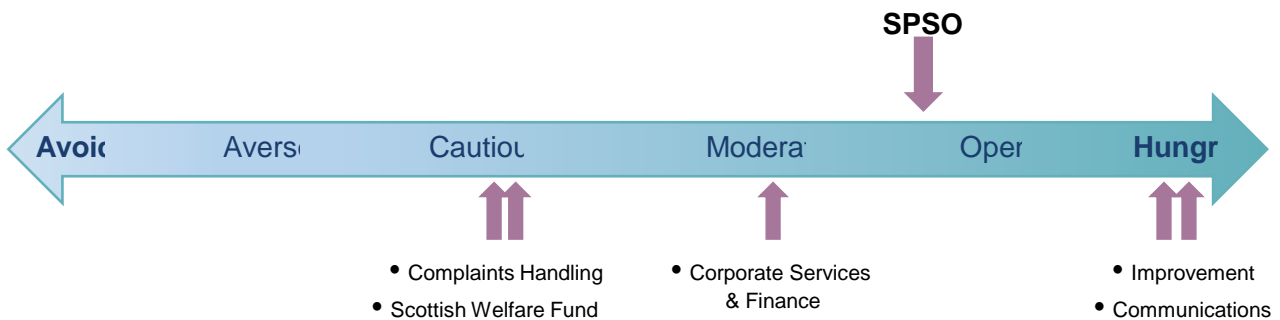
## Introduction

This document sets out the Scottish Public Services Ombudsman's risk management plan in line with the strategic plan and annual business plan for the period. It sets out our appetite for risk and how we assess the risks to achieving our business plan. It should be read in conjunction with our Risk Management and Incident Reporting Policies, in the Governance and Risk Management handbook published on our website here:

[SPSO Governance and Risk Management Handbook](#)

## Risk appetite

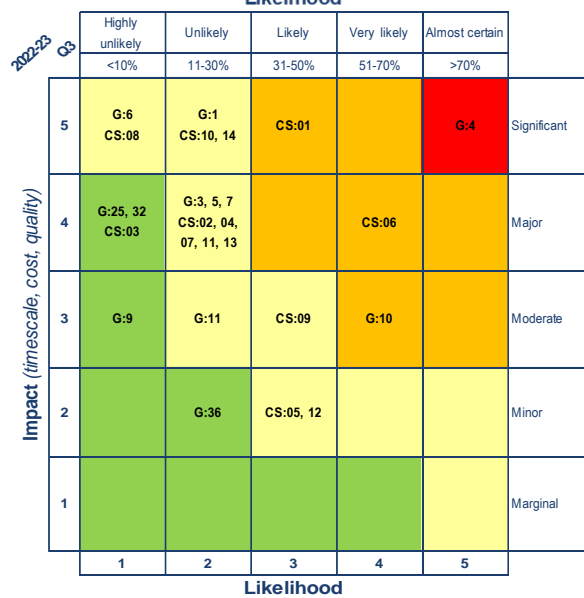
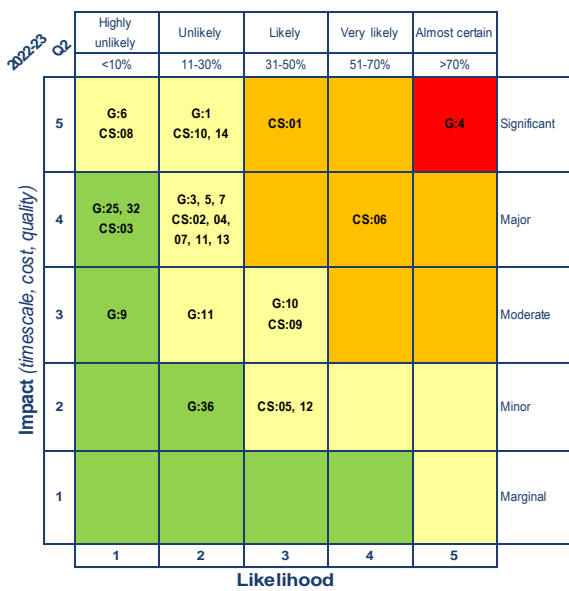
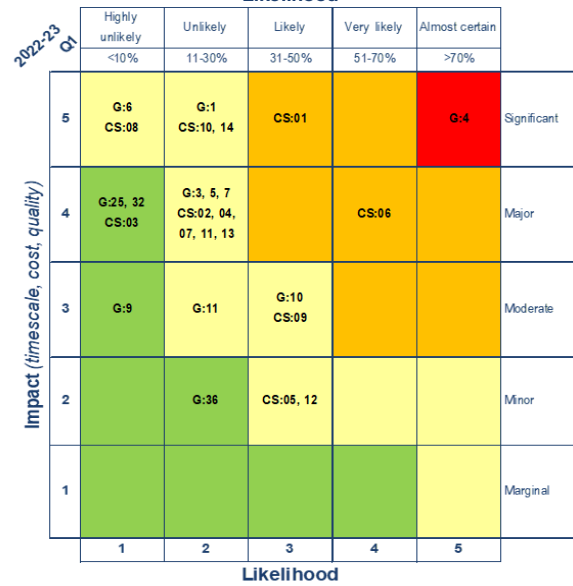
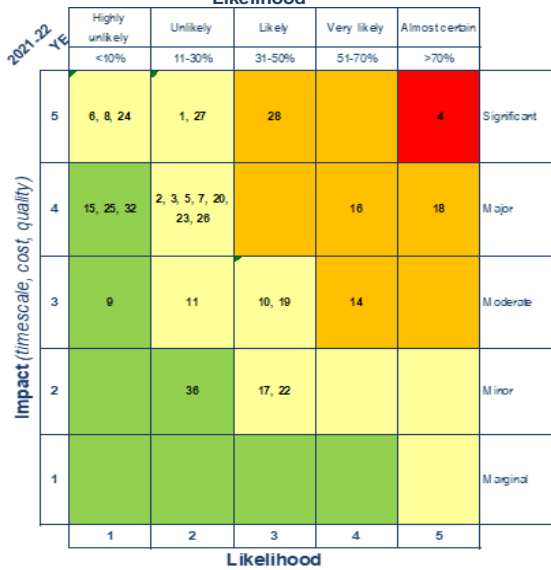
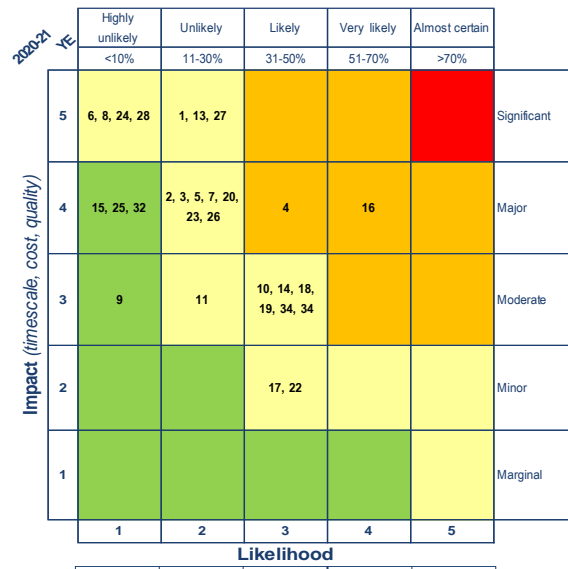
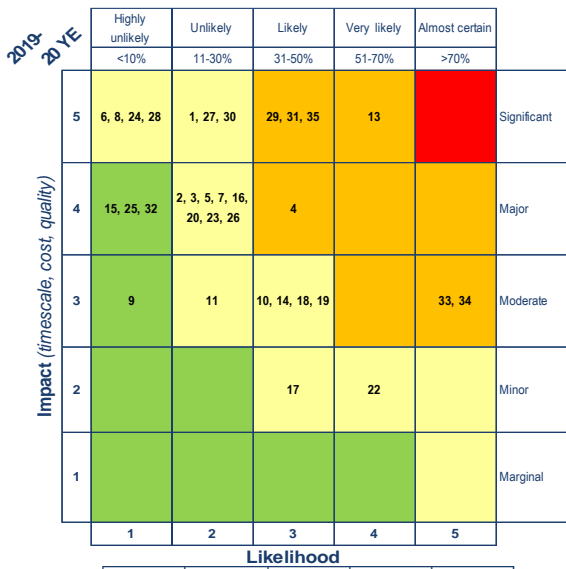
Our current overall risk appetite is defined as 'Open'. This means the SPSO will continue to encourage new thinking and invest in people, systems and processes that will enable the organisation to achieve continuous improvement in the quality and user-focus of our services.



# SPSO Risk Register

## Scattergram of operational risks

The scattergrams below show the spread of operational risks following the quarterly review



SPSO Risk Register

Risk nos.	Description of area of risk	Strategic Objective	Risk owner	Inherent Likelihood	Inherent Impact (time, cost, ...)	Inherent score	Control action in place (Further mitigation actions through the annual operations risk registers)	Current likelihood	Current impact (time, cost, ...)	Current Score	Current Status	Management response
SR1	If the SPSO does not maintain and develop further their positive reputation for effectiveness, efficiency, transparency and excellence it will undermine stakeholder relationships, and damage our standing as world-leading experts.	Accessibility Access to Justice Capacity Standards	SPSO	3	5	15	L: Strong governance and innovation structures in place through for example the scheme of control, robust quality assurance processes, active member of Ombudsman's networks, regular engagement with the parliament.  I: Strong body of work published, open and transparent governance, engaging with the Scottish Government to deliver improvement practices.	2	3	6	Open	Tolerate
SR2	If the SPSO does not communicate clearly and openly about our role and remit, and the positive impact of our work, this will undermine public support, trust and confidence in our service, and inhibit our ability to drive public sector improvement	Accessibility Access to Justice Standards	SPSO	3	5	15	L: Strategic and annual business plans; proactive stakeholder engagement strategy; annual report; regular review of communications tools (web, leaflets, e-newsletter); sounding boards; tracking media coverage and e-newsletter open rates  I: Acting on feedback from surveys, customers and sounding boards; regular meetings with SPCB; investing in relationships with key Scottish Parliament, Government and third sector stakeholders.	1	3	3	Open	Tolerate
SR3	If we do not have in place, maintain and apply robust governance systems, clearly linked to output and performance, we will be unable to deliver and demonstrate value for money, effective and efficient service, and not meet all our statutory duties.	Accessibility Capacity	SPSO	2	5	10	L: Strong governance structures in place through the scheme of control, internal and external audit plans.  I: Strong relationship with the Scottish Parliamentary Corporate Body	1	2	2	Open	Tolerate
SR4	If we have inadequate funding and resources, and do not maintain and develop capacity where and to the standard needed, our work plan will not be delivered by sufficient, motivated, skilled and supported colleagues to time and quality standards set.	Accessibility Capacity	SPSO	5	5	25	L: Approach to resourcing outlined in the Strategic Plan, fully engaged in budget bid process, careful consideration of resource requirements through business planning process, engagement with staff representatives  I: Corporate communications, support for managers having difficult conversations, learning and development plan includes staff wellbeing.	4	5	20	Open	Treat
SR5	If we cannot maintain business continuity due to a cyber incident or other external factors outside our control (at local, national and international level) and do not have effective contingency plans, this may result in systemic delivery and resourcing issues, we will be unprepared and unable to meet our statutory functions and deliver our strategic plan.	Accessibility Access to Justice	SPSO	5	5	25	I: Business Continuity Plan reviewed regularly with appropriate testing and liaison with third parties. Cyber resilience plan in place, CR accreditation confirmed with major contractors; LT and ISA to attend relevant briefing sessions and remain informed of the risk and implement appropriate protections; L: Agree approach in relation to disruption to business. Monitor external sources of information and act on plans as needed.	4	4	16	Open	Treat
SR6	If the UK or Scottish governments introduce policies or take decisions that have significant negative impact on the delivery of Scottish public services, this may result in systemic delivery and resourcing issues across the public sector, SPSO included, impacting on our ability to meet statutory duties.	Accessibility	SPSO	4	5	20	I: LT and LPO horizon scan, monitor developments and attend briefing, information and discussion sessions, maintain a particular focus on post BREXIT, devolved and non-devolved matters, and wider economic policies. Monitor internal impact and respond to Scottish Government (and where appropriate UK Govt) impact surveys	4	5	20	Open	Treat
SR7	If SPSO fails to understand and adapt to the threats and opportunities posed by climate change, then this may lead an inability to meet our statutory duties, reputational damage, environmental damage and potential financial penalties.	Accessibility Access to Justice Capacity Standards		5	5	25	Climate Change and Green group to horizon scan, monitor developments and keep LT updated. SPSO is developing a Climate Change Strategy that will plan and control this risk. Progress towards the Strategy and associated actions is managed through the Climate Change and Green group.	3	3	9	Open	Treat

# SPSO Risk Register

## Introduction

The Scottish Public Services Ombudsman recognises that assessing the level of risk it accepts will help the organisation achieve its aims of delivering beneficial outcomes to its stakeholders.

The SPSO aims to balance the methods it uses to control risks so it can both support innovation and the imaginative use of resources and continue to provide a best value public service. The SPSO will seek to control all probable risks which have the potential to:

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

The organisation's current overall risk appetite is defined as **OPEN**. This means the SPSO will continue to encourage new thinking and invest in people, systems and processes that will enable the organisation to achieve continuous improvement in the quality and user-focus of our services.

## Descriptors

AVOID	No appetite. Not prepared to accept any risks.
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.
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.
MODERATE	Tending always towards exposure to only modest levels of risk in order to achieve acceptable, but possibly unambitious outcomes.
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.
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.

## Appetite for each function

<i>Function</i>	<i>Appetite</i>	<i>Detailed statement</i>
Complaints handling service	CAUTIOUS	We will accept only low levels of risk that could undermine our provision of systems and processes that enable us to achieve continuous improvement in the quality and user-focus of our services.
Scottish Welfare Fund service	CAUTIOUS	We will accept only low levels of risk that could undermine our provision of this new service in an efficient and high-quality manner.
Improvement activities	HUNGRY	We will seek and implement innovative and pioneering approaches to support learning and improvement by Scottish public services; and will encourage new thinking and ideas that could enable us to help service providers to improve their complaints handling.
Communications	HUNGRY	We will seek and implement innovative and pioneering approaches to engage effectively with our Stakeholders to ensure a good understanding of the SPSO is achieved.
Corporate Services	MODERATE	We will accept only modest levels of risk as is reasonably possible in relation to our financial position and the probity of our governance arrangements

# SPSO Risk Register

**Policy:** SPSO - Governance and Risk Management

<https://erdm.scotland.gov.uk:8443/documents/A27617085/details>

## Overview

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. 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. 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.

## Roles and Responsibilities

**Leadership Team:** Through a process of corporate evaluation of the known risks, the LT compiles an overall list 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.

**Management Group:** Managers consider operational risks in the performance management meetings, with any updates reported through the LT representative.

**All staff:** Additionally, all papers submitted to the LT for consideration during the course of the business year must be accompanied by a cover paper that includes a reference to the annual business plan and relevant risk.

## Review

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

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

The strategic risk register is discussed with the AAB at each meeting.

## Risk Evaluation and Response

1. 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
2. The overall significance of the risk is then rated as low, medium, high or critical.
3. The controls currently in place are detailed, identified as L: for those changing the likelihood score and I: for those changing the impact score. The risk is re-assessed with a current score.
4. Consideration is given to the business tolerance for the risk and a target score for each risk is agreed.
5. Any further planned controls to mitigate the risk and reach the target score are recorded, and the business plan action identified.

### Risk level

<b>21-25 = Critical</b>	Unacceptable level of risk exposure that requires immediate mitigating actions.
<b>12-20 = High</b>	Unacceptable level of risk that requires controls to be put in place to reduce exposure.
<b>05-10 = Medium</b>	Acceptable level of risk exposure subject to regular active monitoring.
<b>01-04 = Low</b>	Acceptable level of risk subject to regular passive monitoring.

# SPSO Risk Register

## Response to Risk

Once the key risks have been identified and assessed, the LT consider how to manage them. Response to risk can be to:

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

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.

## Glossary of Risk Categories

This list summarises the most common types of risk and some indication of the possible effects:

Infrastructure: *utilities, suppliers, business relationships, dependency on internet and email*

Budgetary: *availability and allocation of resources*

Legal & Regulatory: *e.g. health and safety legislation*

Political:

*possible political constraints like a change of government*

"Act of God": *fire, flood, earthquake*

Policy: *appropriateness and quality of policy decisions*

Operational: *procedures employed to achieve particular objectives*

Information: *adequacy of information used for decision making*

Reputational: *public reputation of the organisation and/or executive and consequent effects*

Transferable: *risks that may be transferred, or transfer of risks at inappropriate cost*

Technological: *use of technology to achieve objectives*

Project: *project planning and management procedures*

Innovation: *exploitation of opportunities to make gains*

Personnel: *availability and retention of suitable staff*

Health & Safety: *well-being of people*

Fraud or theft: *unproductive loss of resources*

Insurable: *potential areas of loss that can be insured against*

Liability: *the right to sue or be sued in certain circumstances*