Risk Management Policy

Descriptor	Changes made	Date	Version
Policy first implemented	Policy prepared in line with good practice.	16.01.2020	1.0
Review no.1	Policy reviewed in line with schedule.	15.03.2022	2.0
Review no.2	Policy reviewed in line with schedule, updates made addressing internal audit recommendations and in line with evolving good practice.	15.09.2023	3.0
Review no.3			

Name of policy being superseded (if applicable)	N/A
Related policies	Code of Conduct
Related SOPs	
Related Guidance	Risk Management Strategy 2022
Equality Impact Assessment completed	No
Island Community Impact Assessment completed	No
Intended Audience	Internal Staff and Key External Stakeholders
For publication	Internally and Externally
Team responsible for policy	Finance
Policy owner contact details (email)	Peter.Burns@sds.co.uk
Policy due for review (date)	September 2025

Policies should have a clear purpose and perform at least one of the following functions. Please identify all the functions this policy performs.	**If statement applies, please mark with an X below**
Outline how we allocate limited resources to deliver services or outcomes	
Outline how SDS adheres to legislation, statutory duty etc.	x
Ensure fair and consistent allocation of benefits	
Protect organisational assets, including data	
Define expectations around the employee/employer relationship	
Other (please specify)	

Contents

1. Policy summary

The risk management policy establishes expectations for how risks to the delivery of performance and objectives will be managed to ensure that SDS can meet its obligations. It also sets out roles and responsibilities for risk management.

2. Policy purpose and objectives

The Scottish Public Finance Manual (SPFM) is issued by the Scottish Ministers to provide guidance on risk management. It gives guidance on the basic principles of risk management which SDS follows through this policy. The guidance is aimed at all organisations to which the Scottish Public Finance Manual (SPFM) is directly applicable.

This policy sets out the key elements of SDS's governance structure and highlights how risk management and assurance activities operate within SDS. This policy highlights that risk management is part of SDS's management function.

3. Strategic context

Risk is unavoidable but SDS manages its risks to remain effective and to operate with efficacy. To support this, SDS has a set of risk management processes and procedures which support and enhance the way we manage the business.

The implementation of this policy helps SDS identify and manage internal and external risks, and provide good corporate governance, which will help achieve our strategic and operational objectives.

Our approach aims to ensure that good organisation-wide risk management will lead to stronger organisational resilience. This will also help colleagues understand the scope of the environment in which they operate and provide them with realistic boundaries for executive action.

The policy has been developed with the support of risk owners across SDS, and follows ISO 31000 principles and guidelines, standards devised from HM Treasury Orange Book principles, National Audit Office report on Managing risks in government, GAD's practical guide to strategic risk management, Chartered Institute of Public Finance and Accountancy (CIPFA), internal audit recommendations and the Scottish Public Finance Manual.

4. Definitions

The following key terms are used within this policy.

Risk Management: activities taken to address the risks attached to delivering SDS strategic and/or operational objectives.

Internal Audit: The shared internal audit function (SE, SDS, SFC & SOSE) provides independent, objective assurance and consulting service on SDS's internal control system.

Risk Category: This should identify the strategic area that may be jeopardised if the risk is not mitigated and must be categorised as either a Strategic, Financial/Operational, Cyber/Data, or People Risk.

Risk Appetite: The risk appetite is the total level of risk that an organisation is willing to expose itself to which reflects the context and changing environmental factors in which it operates.

Risk Management Process: The systematic application of management policies, procedures, and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring, and reviewing risk.

Assurance: When one party wishes to take comfort over a subject matter prepared by a second party, and the assurance is only provided when a third party can provide an independent perspective.

A full list of definitions and a glossary of terms are available here.

5. Scope

The Risk Management Policy (the Policy) applies to all employees. In addition, the Policy extends to non-employees such as contractors, and third part suppliers engaged to deliver services on our behalf, those who use our services and other parties who may be affected by our activities.

6. Policy detail

We shall implement the risk management framework for assessing risks, evaluating both the likelihood of the risk being realised and of the impact if the risk is realised. Risk assessment should be recorded in a way that demonstrates clearly the key stages of the process.

We shall integrate risk management as a key element of the integrated business planning process. The approach shall be tied to the organisation's purpose and objectives through T27, integrated work plans and the strategic plan.

We shall deploy a systematic approach for identifying risks and maintaining a clear record of risk in Ideagen Risk Management.

We shall review risks regularly to monitor whether or not the risk profile is changing, to gain assurance that risk management is effective, and to identify when further action is necessary.

We should clearly describe and prioritise risks in relation to objectives with a risk description combining both the possible cause and impact to the objective.

We shall assign all risks, once identified, to an owner who has responsibility for ensuring that the risk is managed and monitored appropriately.

We shall maintain effective communication and raise awareness about potential problems and share important information to aid better problem solving, provide effective challenges and support effective escalation.

We shall determine the risk appetite to deliver effective risk management and to support decision making and how risks can ultimately be addressed.

We shall use Ideagen Risk Management for recording, monitoring, and reporting purposes. The recording of material and key risks not in Ideagen Risk Management shall be avoided as this inhibits governance arrangements and restricts the communication of risks across the business, including sharing lessons learned and good practices. Where a risk has a high or medium risk exposure the risk owner shall identify an action to mitigate.

6.2 Roles and Responsibilities

SDS Board
The Board's Terms of Reference (ToR) states that its strategic responsibilities is to "ensure that the Board maintains strategic scrutiny of corporate risks and SDS risk management". This should include a regular review of the risk management framework.

Audit and Risk Committee (ARC)
Audit and Risk Committee Terms of Reference (ToR) states that its responsibilities are to "consider the strategic process for risk, control and governance and the Statement of Internal Control".

Accountable Officer
The memorandum to accountable, states that the Accountable Officer (CEO) is responsible to "ensure that risks, whether to achievement of business objectives, regularity, propriety or value for money, are identified, that their significance is assessed and that systems appropriate to the risks are in place in all relevant areas to manage them".

Executive Governance Board (EGB)
The EGB Terms of Reference (ToR), states that it shall "provide oversight for financial management, HR establishment and workforce development planning, health and safety, risk, SDS policies and business assurance matters". Furthermore, it "will consider and make decisions on these matters with ultimate accountability for management of the financial resources as a whole and for corporate governance and compliance".

EGB shall provide the mandate and commitment to manage risk, and support governance arrangements.

Directors and Heads of Service
Directors and Heads of Service are accountable for implementation and compliance with the Policy, in respect of all their business activities, across their Directorate/areas of responsibility. Directors and Heads of Service have a responsibility to:

- demonstrate visible commitment to risk management and corporate governance
- provide leadership for risk management, promoting risk management proactively throughout their Directorate/areas of responsibility

- adequately deploy resources to effectively implement this Policy
- review risk management performance on a regular basis, directing action where required
- assure their governance board that the Policy is fully complied with.

Risk and Internal Audit Manager

The Risk and Internal Audit Manager is appointed by the Director of Finance, Information Governance, Resilience and Risk as the primary 'competent person' for risk management matters. The Risk and Internal Audit Manager is responsible for:

- supporting the business to properly identify, understand, and manage risks across all levels within the organisation
- developing and deploying the risk management framework
- developing and progressing the risk management strategy and related guidance
- defining the content of this Policy, and updating as necessary
- defining the content of supporting policies, and procedures, and updating as necessary
- providing advice on risk management matters, including learning materials and guidance on the interpretation of this Policy
- defining the minimum required compliance information / metrics that should be used to continually evaluate compliance, and collating and reporting as appropriate
- establishing and implementing a programme of quality assurance to evaluate compliance with SDS' risk management approach, and recommending action required to meet the required standards
- coordinate governance arrangements and formally recording the business's commitment to managing risk, governance arrangements, training, resources, and processes
- reviewing the overall risk management process to deliver assurance that it remains appropriate and effective.

Risk Owners

Risk Owners are responsible for identifying and managing the risks that have an impact on their objectives, to ensure all risks are recorded and that the actions taken to mitigate them are correctly recorded in Ideagen Risk Management.

Risk Coordinators

Risk Coordinators are nominated contacts for each Directorate or team to support the Director and Heads of Service with the management of risk. The Risk Coordinator provides support to update risks held in Ideagen Risk Management and provide guidance and support to individual risk owners. Risk Coordinators support the Risk and Internal Audit Manager by holding monthly meetings to ensure risks, actions and internal controls are prioritised and to highlight any gaps and inconsistencies within the recording of the risks in their area. A nominated Risk Co-ordinator must be in place for each directorate or team to support the Director and relevant managers to fulfil their risk management responsibilities.

Specialist Risk Teams

Specialist functions (Business Continuity, CPMO, Health & Safety and Information Security) are in place to manage specific types of risk, and these provide the Board and management with assurance in these areas.

6.3 Governance Arrangements

Clear governance arrangements shall continue to underpin the SDS Risk Management Framework.

SDS Board

The SDS Board shall monitor arrangements in place to provide assurance on risk management, governance, and internal controls.

ARC

ARC shall monitor the Corporate Risk Register to allow it to consider the adequacy of arrangements for the assessment and management of risks, with a particular focus on the corporate risks which are presented by the Risk and Internal Audit Manager on behalf of SDS. ARC considers assurances relating to the corporate governance requirements for SDS.

EGB

EGB shall monitor levels of assurance over the management of Strategic Risks and the quality of risk management across the business.

Portfolio Leads

The Portfolio Leads should undertake a thorough review of the corporate risks and portfolio change and business as usual risks and review the risk appetite for each category of risk. Portfolio Leads provide recommendations on the escalation, de-escalation, and closure of strategic level risks.

Portfolio Leads shall provide a risk assurance statement, annual internal controls checklist and a certificate of assurance to confirm to the Accountable Officer that risk arrangements and controls are working as intended in their areas.

Quality Assurance of the management of risks will be communicated to the relevant Portfolio lead by the Risk and Internal Audit Manager.

Directors/Heads of Service

Arrangements to support the management and control of risks within relevant business areas should be reviewed through team meetings, project/programme board meetings, topic specific meetings and governance meetings. They should provide and seek assurance that the policy is followed.

Risk owner

Risk owners shall review their risks and update the status of the risks and progress of their action plans monthly in Ideagen Risk Management.

Risk and Internal Audit Manager

The Risk and Internal Audit Manager should seek assurance that operational risks are reviewed, actions and internal controls are robust and identify any gaps and inconsistencies in the recording of the risks in Ideagen Risk Management.

6.4 Risk Reporting

Risk reporting is a key component of an effective risk management framework. To fulfil its responsibilities as outlined in Committee/Group ToR, the Board, and specifically the ARC, shall report strategic and operational level risks. Risk management papers presented to the ARC shall include a report on SDS strategic risks.

Risk management reporting within SDS includes a range of risk management KPIs and trend analysis that enhances oversight and assurance.

The EGB shall be provided with a regular risk management report on strategic and organisational risks. EGB should conduct an annual assessment of future corporate risks including horizon scanning with findings communicated to ARC and EGB.

Directorates and teams should regularly review, monitor and report on their risk registers (supported by the risk management function) to ensure that risks are identified and escalated to the appropriate level at an early stage.

6.6 Risk Appetite

The SDS risk appetite is based on a considered view of organisational risks, issues, and consequences. Appetite levels vary according to the category of the risk. SDS will always aim to operate organisational activities at the levels defined below.

The risk appetite scale that SDS uses below are based on successful practice collated from the Civil Service Risk Community.

Risk Appetite	Description
Opposed	Avoidance of risk and uncertainty in achievement of key deliverables or initiatives is a key objective.
Minimal	Preference for very safe business delivery options that have a low degree of inherent risk.
Cautious	Preference for safe options that have low degree of residual risk.
Mindful	Willing to consider all options and choose one most likely to result in successful delivery.
Enterprise	Eager to be innovative and to choose options that suspend previously held assumptions and accept greater uncertainty.

SDS has defined five key risk categories which is supported by a risk appetite statement:

- Strategic Risks
- Finance/Operational Risks
- People Risks
- Cyber/Data Risks
- AI/emerging technology Risks

6.7 Continuous Improvement

The Orange Book and the Risk Management section of the Scottish Public Finance Manual both emphasise the importance of continuous improvement around risk management and sharing learning and experiences from managing risks at various levels across the organisation.

The UK Government Function “Good practice Guide – Risk Reporting” states that the Board, supported by ARC, should periodically review the quality of reporting, and provide feedback on the scope, purpose, and content of reports. The good practice guide further notes that reporting should also be reviewed in response to changes to the operating environment, shifts in the risk culture or changes to organisational risk maturity. Other events which provide opportunities to develop and embed the delivery of quality products supporting informed decision-making and organisational oversight should also be considered.

Whilst there have been no specific instances, there is an opportunity to further improve SDS’s risk management arrangements through formal “lessons learned” sessions if a significant, unforeseen risk materialises, or where stated mitigants were ineffective. A consideration of lessons learned will help to further embed continued learning and development within SDS’s risk management arrangements.

7. Further guidance

Colleagues are referred to the **Connect** policy site for guidance and Policies around the associated policies referred to in this policy.

- Risk Management Framework
- Risk Management Strategy
- Risk Management Process
- Risk Management Guidance
- Risk Management Ideagen user Guidance
- Risk Management and Internal Audit Connect Page
- Risk Management and Internal Audit Microsoft Teams Page
- Internal Audit Mission and Charter
- Scottish Public Finance Manual
- Orange Book
- SDS Corporate Strategy
- Definitions and Glossary