Somerset Council

Risk Management Guidance

Draft October 2024

Appendix 4

Contents

Risk Management Guidance

Risk Management Cycle

Step 1: Identifying Risks and Opportunities (and Recording)

Risk identification is the first step in the management process.

The starting point for the identification of risks is to identify the outcomes that are to be achieved. This may be obtained through the examination of key priorities, directorate / service business plans or project / programme objectives. The risk to the delivery of these outcomes can then be identified.

It is important that risks are correctly described to ensure they are fully understood, and appropriate actions identified. Risks needs to be described in clear terms that can easily be understood.

Risk descriptors are often prefaced with one of the following:
'**Lack of…' 'Loss of…' 'Failure to…' 'Inability to….' 'Reduction of…' 'Disruption to'**

Risks should generally be described in a couple of sentences, explaining the risk, cause, and consequence.

Example:

Failure to deliver a major change project on time and in budget (risk) due to lack of project management and appropriate resources and conflicting priorities (cause) which will result in detrimental impact to deliver the next stage of the program and will increase temporary staffing costs (effect).

All strategic, service and key project risks, that are required to be recorded (see 'scoring' section later), are to be recorded within the corporate risk management system.

Ideagen is the Council's risk management system for recording, monitoring, and managing those risks that require a management response.

Training in the use of Ideagen for managing risks will be available on request in group or one-to-one sessions. Please contact the Corporate Risk Manager for available dates.

All recorded risks should be categorised under one of the four Council Plan priorities. This will help with consistency of reporting, as corporate performance will also be structured in the same way

Step 2: Risk Analysis (Scoring)

This is the process of reviewing the risks identified and assessing the potential likelihood of them occurring and the impact they would have.

The risk scoring matrix we use is a 5 x 5 grid that guides users through the priority scoring of individual risks by considering Likelihood & Impact.

The initial assessment should consider the inherent or gross risk. This is the potential likelihood and impact of a risks crystallising if no controls are in place. By multiplying one score by the other, the total indicates the perceived risk severity and management level required.

Once the inherent/gross risk has been identified, any controls that are in place to help manage the risk should be identified and any reduction in the likelihood and impact scores identified to give the residual / current risk.

It is essential that any controls that are being relied upon to manage risks are effective. As part of the assessment process the sources of assurance that provide ongoing confirmation that controls exist and continue to remain effective should be identified.
The final stage in the analysis is to consider and set the target risk. This is the level of risk that you are aiming to manage the risk down to. This will help in determining what mitigating actions need to be taken. The Risk Scoring Matrix, on the following page, supports the setting of an appropriate target risk.

The complete risk scoring guidance is available from Risk Scoring Matrix interim 2024-23042024.doc.docx (sharepoint.com)

Step 3: Risk Prioritisation

Once risks have been assessed they can be mapped onto the Risk Scoring Matrix. The colours act as a “traffic light” system that denotes the reporting requirements and overall risk score. The thick black line separating the medium and high risks is the “line of Tolerance”

A comparison of the prioritisation matrix for inherent, residual and target risk will demonstrate how controls have influenced the level of risks and where additional control may be required.

Risk Scoring and Reporting Matrix (RSM)

Likelihood (A)	**5. Very Likely** >90% chance	**5 Low Annual**	**10 Low Quarterly**	**15 Medium Quarterly**	**20 High Monthly**	**25 Very high Monthly**
	4. Likely 50% to 90% chance	**4 Low Annual**	**8 Low Quarterly**	**12 Medium Quarterly**	**16 High Monthly**	**20 High Monthly**
	3. Possible 25 to 50% chance	**3 Low Annual**	**6 Low Quarterly**	**9 Medium Quarterly**	**12 Medium Quarterly**	**15 Medium Quarterly**
	2. Slight Likelihood 10 to 25%	2 Recording of risks at this level is optional	**4 Low At least Annual**	**6 Low Quarterly**	**8 Low Quarterly**	**10 Low Quarterly**
	1. Very unlikely	1 Recording of risks at this level is optional	2 Recording of risks at this level is optional	**3 Low Annual**	**4 Low Annual**	**5 Low Annual**
		Insignificant 1	**Minor 2**	**Significant 3**	**Major 4**	**Critical 5**
		IMPACT (B)				

Step 4: Management of Risk - Risk Response Strategies and Mitigation

For risks recorded in the risk management system, a decision as to the appropriate response is required. The response chosen will determine whether mitigating action is necessary, who needs to be made aware of the risk and how frequently it is reviewed.

Risk Response Strategy

Colour	Score (L x I)	Action	Risk Response
Pale green	1 - 2	**Very Low Risk** - Acceptable risk if the inherent and or current score is at this level no further action or additional controls are required.	**No further action required**
Green	3 - 10	**Low Risk** - Acceptable risk; No further action or additional controls are required; Risk at this level should be monitored and reassessed at least annually. Record in RM system Monitor quarterly to annual	**Tolerate, treat, transfer, or terminate** the activity that leads to the risk
Yellow	9 & 15	**Medium Risk** - A risk at this level may be acceptable; If not acceptable, existing controls should be monitored or adjusted; No further action or additional controls are required. • Record in RM system • Review quarterly	**Treat, Transfer**
Red	16 - 20	**High Risk** - Not normally acceptable; Efforts should be made to reduce the risk, provided this is not disproportionate; Determine the need for improved control measures • Unacceptable - Out of Tolerance • Record in RM system • Review Monthly • Requires immediate Service Director Action • May require escalation to Executive Directors	**Treat, Transfer, Terminate risk activity**
Red	25	**Very High Risk -** Unacceptable; Immediate action must be taken to manage the risk; Several control measures may be required Requires immediate Executive Director Action • Unacceptable - Out of Tolerance • Record in RM system Review Monthly	

Risk Response Methods

Transfer the Risk – a directive control
This is usually possible when the likelihood of the risk happening is 'low' but the impact [if it

did occur] is high, in this instance transferring the risk to another organisation may be the answer. One common way is by purchasing insurance, where the insurer takes on the financial burden in exchange for a premium. It is, however, important to note that not all risks can be insured due to cost of premiums or because the risk is not insurable. Another approach could be to transfer legal liability to another entity through contractual agreements. However, it is important to note that while some risks are transferred, new risks may also be introduced, requiring careful management. Any risk that is transferred still remains the responsibility of the Council with management reviewing the arrangements to assure themselves that all is working as planned.

Tolerate the Risk – a detective control
The Councils readiness to bear the risk after treatment in order to achieve its priorities/objectives.

Following thorough analysis, it may be acceptable to take no action regarding a risk. This can happen when the cost of mitigation is disproportionate to the potential benefit or when the risk is beyond the Council's control, such as legislative changes or external decisions. You should also consider once all available mitigation is in place and where continued monitoring would provide no further benefit if the risk can be recorded as 'tolerated'.

Treat the Risk – a corrective control
The majority of risks fall into this category. Treating the risk involves implementing control mechanisms and mitigation strategies to manage the risk to an acceptable level. If this is a new activity to your service area or the council, you will have 'Proactive' controls' (existing) and will be able to identify 'Reactive' controls (in progress). The goal is not necessarily to eliminate the risk, this may not be a financially appropriate option, but to reduce it to a level where it can be managed effectively.

Terminate the Risk – a preventive control
If an activity is considered to pose too high a risk, the Council may decide to cease the activity altogether or reassess the situation. This involves evaluating whether the activity can be conducted in a different manner or if it should be stopped to eliminate the risk entirely. If the risk arises from a statutory activity, then termination may not be possible, in this instance controls must be proposed and implemented which could include risk transfer.

Step 5: Monitor and Review Risks

This is a key stage of the process and should happen on a continuous basis. It is necessary to regularly report on the progress that is made in managing risks, so that the achievement of the Council's aims, and service objectives is maximised, and negative impacts are minimised.

As part of this process there needs to be an assessment of the effectiveness of risk management actions put in place to reduce the likelihood / impact of adverse risk events occurring. Alternative action should be taken if the initial action has proved ineffective.

Risk Escalation

Identifying when a risk should be escalated is an important part of the monitoring process. There may be instances where the risk owner cannot take further action to mitigate a risk meaning the risk should be escalated to the next management level, a reassessment of the current score will determine if the risk has moved into the 'high'(red) category.

Escalation enables the transferring of ownership and accountability. All officers are responsible for the identification and management of risks, escalation does not necessarily mean that the risk will be adopted at a higher level e.g., strategic, but it does enable consideration of approval for additional mitigation at a higher level.

The table below outlines the escalation route.

Escalation of a risk					
	Service Manager*	HoS/Strategic Manager*	Service Director	PRB BOARD**	Executive
Service Level	☑	☑	☑		
High Scoring Operational (red risks)	☑	☑	☑	☑	
Strategic Level		☑	☑	☑	☑
Programme and Project Risks					
	Project Officers	Project Managers	Programme Manager	Project Board	
	☑	☑	☑	☑	

- *Job titles correct at time of writing. **Performance, Risk & Budget Board

Risk Appetite

To achieve its objectives, Somerset Council must take risks. The Council's Target Operating Model states that our approach is to be risk aware rather than risk averse, managing risks rather than trying to eliminate them. Decisions on which risks to accept or avoid depend on the context, potential losses or gains, and the completeness and reliability of information. As risk appetite is context-driven, the Executive Leadership Team/PRB? will regularly review and approve corporate thresholds to ensure alignment with the Council's strategic objectives and the prevailing risk environment.

Risk appetite is defined as; the level of risk the council is willing to take to achieve strategic priorities. It promotes consistent, 'risk informed' decision-making aligned with strategic priorities, and it also supports robust corporate governance by setting clear risk-taking boundaries.

The Council's risk approach can be classified as:

- **Risk Averse**: Accepts as negligible risk as possible. Not willing to accept any negative impact to pursue objectives
- **Risk Concerned**: Cautious approach to risk taking. Only willing to accept a small negative impact to pursue objectives
- **Risk Tolerant**: Greater than normal risks are tolerated. Willing to accept some negative impact to pursue objectives
- **Risk Seeking**: Aggressive risk taking is justified. Willing to accept a significant negative impact to pursue objectives
- **Risk Open**: Willing to consider all potential options and choose the one most likely to result in successful delivery, while also providing an acceptable level of reward and value for money.
- **Risk Neutral**: Balanced risk approach. Potential negative impacts and objectives competition are given equal consideration.

The Council's risk appetite varies by circumstance. Generally, the Council seeks to be innovative and continuously improve within a framework of compliance, value for money, and strong governance. Robust risk management at all levels aims to encourage a less risk-averse and more risk-aware approach, fostering innovation and opportunity within the Directorates while managing barriers to success. However, attitudes toward risk will differ, with a lower appetite for risk in areas such as legal compliance and safeguarding.

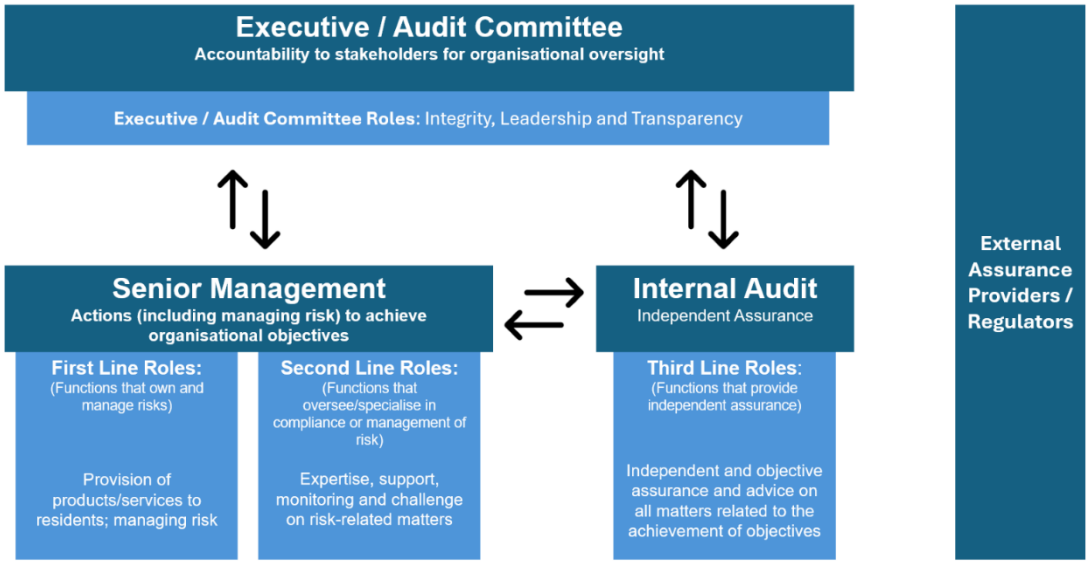
Reporting and Monitoring

The reporting hierarchy for risk and the associated review bodies are included in the table below:

Risk reporting	Review body
Quarterly - Strategic/ HSOR Risk Registers Updates and provides assurance to the Audit Committee on the Council's strategic & HSOR risk registers,	**Audit Committee**
Quarterly- Strategic/ HSOR Risk Register Strategic/ HSOR risk register – cross cutting risks that could have a significant impact on the Councils' operations.	**Performance Risk & Budget Board**
Directorate HSOR Risk Register High scoring operational risks that impact on the objectives of the directorate and its services. Risk associated with project and programmes within the Directorate.	**Directorate Management Teams**
Service, operational and programme / project risks Risks directly impacting on the service, operation, or programme / project delivery.	**Service/Operational Management Teams** **Programme & Project Boards** **H&S Committees**

Detailed Roles and Responsibilities

The Three Lines model helps identify and understand the contributions of various sources of assurance:



Adapted from The Institute of Internal Auditors 2020

Role	Responsibilities
All Councillors	• Ensure that risk considerations are part of the decision-making process, weighing potential risks and benefits before making decisions. • Challenge reports that contain inadequate consideration of risk, • Participate in risk management training. • Hold the ELT and other council staff accountable for implementing and maintaining effective risk management practices.
Audit Committee	• Review and approval of the Council's Risk Management Framework, • Regular review of the Council's Strategic Risk register and the status of mitigating actions, • Provide guidance and recommendations on the Council's risk management processes and procedures, • Provide constructive challenge to our management of risk.
Performance Risk and Budget Board (PRB Board)	• Regularly review the Strategic Risk Register to ensure appropriate mitigation is in place, and to challenge where further mitigation is necessary, • Consider the response to high-scoring operational risks that have been escalated, • Allocate owners for effective risk management of strategic risks, • Scan for new strategic risks to the council, • Set the Council's risk appetite and tolerance levels,

	• Own the Risk Management Framework, approve changes to it, and keep its effectiveness under review, • Consider recommendations from the Audit Committee in relation to risk management.
Chief Executive	• The Council has effective and efficient risk management arrangements in place. • All decision-making is in line with Council policy and procedures for management of risk and any statutory provisions set out in legislation. • Adequate resources are made available for the management of risk. • Management of risk performance is continually reviewed. • The risks facing the Council and the County are understood. • Raise the profile of risk management by supporting and promoting a risk management culture and ensuring that everyone is aware of their responsibilities and accountabilities.
Executive Leadership Team (ELT)	• Play an active role in the management of strategic risks as part of the PRB Board, • Take ownership of strategic risks allocated to them, • Set the tone. Advocate the importance of risk management across their areas of responsibility; • Have a clear understanding of the most significant risks affecting their areas of responsibility and an up-to-date awareness of the action that is being to mitigate those risks. • Ensure risk is regularly discussed within team meetings. • Escalate high scoring service delivery risks within their areas of responsibility where mitigation cannot be achieved within the directorate's resources or span of control.
Strategic and Service Managers /Heads of Service	• Ensure risk management policies and procedures are implemented within their service areas. • Consider appropriate responses to risk identified through independent assessment such as External Audit inspections and reviews, Commission for Social Care Inspection, Ofsted etc. • Actively identify and assess risks specific to their departmental operations and projects. • Develop and oversee the implementation of risk mitigation plans within their areas of responsibility • Allocate risk owners and resources necessary to manage risks within their areas of responsibility. • Monitor and address partial audit recommendations resulting from Internal Audit reports. • Ensure that all service level and project risks are recorded, and that regular monitoring and review takes place. • Discuss the risks for their service area at management meetings to gain assurance that the risks are being managed down to an acceptable level. • Escalate high scoring service delivery risks within their areas of responsibility where mitigation cannot be achieved within their resources or span of control. • Ensure any reports written by officers in their service areas, to Council or it's Committees, include thoughtful and appropriate reference to risk. • Advocate the importance of risk management across their areas of responsibility.
IT and Data Security Staff	• Protect Data: Ensure the security of the council's data and IT systems against cyber threats. • Monitor Systems: Continuously monitor IT systems for vulnerabilities and breaches. • Data Recovery: Develop and maintain data recovery plans in case of system failures or data loss.
Financial Officers	• Financial Controls: Implement financial controls to prevent fraud, mismanagement, and financial losses.

	• Risk Assessment: Regularly assess financial risks and develop strategies to manage them. • Budgeting: Include risk management considerations in budget planning and financial forecasting.
Health and Safety Officers	• Safety Training: Develop and implement health and safety training, and awareness, to mitigate workplace hazards. • Training: Conduct regular training sessions on health and safety protocols for all staff. • Incident Investigation: Investigate incidents and accidents to identify root causes and recommend preventive measures.
Human Resources (HR)	• Policy Enforcement: Ensure that HR policies support risk management objectives, including recruitment, training, and performance management. • Employee Training: Provide training on risk management and compliance issues. • Incident Response: Manage HR-related incidents, such as workplace disputes or misconduct, in a way that minimises risk.
Internal Audit Staff	• Review Processes: Conduct regular audits of risk management practices to ensure compliance and effectiveness. • Identify Gaps: Identify areas where risk management practices can be improved. • Report Findings: Report audit findings to the risk manager and council leadership.
All Members of Staff	• Follow established risk management procedures in their daily tasks, • Report any identified significant risks to their supervisors/line managers, • Ensure compliance with relevant regulations, policies and safety standards in their work activities. • Participate in risk management e-learning.
Corporate Risk Function	• Provide professional advice on all aspects of risk management, • Develop and maintain risk managements procedures and systems that align with best practice. • Review the effectiveness of the council's risk management arrangements; escalating issues or recommendations to the appropriate level of the organisation. • Draft strategic risk management reports for the Audit Committee and PRB Board; extracting the most recent information from the council's risk management system to support those reports. • Help facilitate the work of the Risk and Performance Community of Practice • Provide training and non-staff resources on risk management practices, promoting a culture of risk awareness and proactive management. • Manage access to the Council's risk management system. • Set up reminders/alerts to ensure that updates are made by risk owners to the corporate risk management system in a timely manner, that fits in with corporate reporting cycles. • Work with the supplier to ensure the risk management system continues to meet the needs of the council. • Implement activities designed to integrate risk management into the overall culture of the organisation. • Horizon scan and network, so that best practice can be adopted within the council. • Work with colleagues to ensure corporate reporting on performance, risk and budget are aligned and cross-reference each other.
Risk and Performance Community of Practice	• Contribute to the development of risk management procedures, • Monitor existing and suggest, emerging strategic risks to the PRB Board, • Share best practice, • Act as Directorate Risk & Performance Champions, • Provide advice, and signpost to colleagues within their directorate to risk management resources,

	• Assist with the role out of changes to risk management systems or procedures, • Help ensure consistency of risk management across the organisation.

Awareness and Training

To implement risk management effectively, all Council members and officers must understand and embrace the Council's risk management approach as part of their responsibilities. This includes embedding risk management into their thinking, behaviours, and actions. Providing clear roles, responsibilities, and reporting lines, along with the necessary knowledge, skills, and awareness, is crucial for effective risk management.

- Risk training for Members is part of the Member Development Programme.
- Annual risk training takes place for Audit Committee Members
- Training for Strategic Managers and Service Managers is provided to prepare them for risk assessment of their services and raise awareness of what is required of them in relation to risk management.
- Individual or group training is available on request.
- eLearning will being developed and will be made available via The Learning Centre
- Risk Management Induction training is available on request
- Risk management system user guides are available.
- System User Training will be available on request.

A Risk and Performance Community of Practice, with membership drawn from across the organisation to ensure wide representation that can provide a support network for risk management matters, sharing good practice and problem-solving. These diverse methods aim to ensure comprehensive understanding and consistent application of risk management practices across the Council.

Risk Registers

The councils risk management system acts as a repository for all risks across the council. With the use of a 'portal' it is possible to bring relevant data together to form an overview of strategic, operational or programme/project risks. For an overview of a Directorates risks you can view the collective data via a Group Portal.

Using the risk register template available from the system, you can print out your risks for submission in committee reports etc.

Risk Register	Description
Strategic Risk Register	Strategic risks are those of significant, strategic, and cross cutting importance that require attention from the councils most senior managers and elected members.

High Scoring Operational Risks	Directorate risks are those that required the attention of the respective Directorate Management Team and have a current score of 16 or more (red)
Service Risk Register, including service managed projects	Service risks are those that required the attention of the respective Service Team, overseen by the relevant service manager/Head of Service. Service risks may be local versions of the corporate, directorate or project risks i.e., specifying in more specific terms how the service and teams will manage the risk as it relates to services
Corporate Project / Programme Risk Register	Project and programme risks will be identified by the Senior Responsible Officer supported by the Performance Management Office (PMO) and owned by the relevant Board.