East Devon District Council

Risk Management – Policy and Guidance

Issue details	
Title:	**Risk Management – Policy and Guidance**
Version number	**Version 3.1**
Officer responsible:	**Simon Davey, Director of Finance and Section 151 Officer**
Authorisation by:	**Audit & Governance Committee**
Authorisation date:	**December 2023**

1   Previous Policies/Strategies

This policy/guidance updates the Risk Management – Policy and Guidance v1.0 January 2012 and September 2014

2   Why has the council introduced this policy?

2.1   This policy and guidance is intended to provide a framework for the management of risk, to increase overall awareness of risk throughout the council and to enable managers and those responsible for risk reporting, to better identify, assess and control risks within their areas. It seeks to enforce ownership. It defines roles and responsibilities to help ensure the risk management process is understood. It gives advice and guidance on best practice and describes the different elements that need to be managed in order that risk management methodology is embedded in every layer of the council.

2.2   We recognise that there are risks involved in everything we do and that we have a duty to manage these risks. This duty is to staff, residents and people working in the district, service users, partners and funding agencies.

2.3   Risk is part of everyday life. It can be defined as the chance that something will happen that has an impact upon aims and objectives. It is recognised that risk management is as much about exploiting opportunities as it is about managing threats, a certain amount of risk taking is inevitable and essential if we are to achieve our objectives. Risk needs to be managed rather than avoided and consideration of risk should not stifle innovation. Risks need to be identified and managed not simply avoided. A key consideration in balancing risks and opportunities, supporting informed decision making and preparing tailored responses is the conscious and dynamic determination of the Council's risk appetite to consider the balance of risk and opportunity.   A separate Risk Appetite Statement supports this policy to assist in the appropriate control of risk.

2.4   This document demonstrates our commitment in taking responsibility to manage our risks and opportunities in all aspects of service delivery effectively, using a structured and cost effective approach.

2.5   We will use risk management to maintain and improve the quality of services within the district and to deliver our priorities and objectives.

Our risk management policy objectives are to:

  ▪ Embed risk management into our culture
  ▪ Raise awareness and work with partners, providers and contractors to develop a common understanding of our expectations on risk management
  ▪ Integrate risk management into policy, planning and decision making
  ▪ Enable us to anticipate and respond to changing social, environmental and legislative conditions

These objectives will be achieved by:

- Identifying, assessing and effectively managing strategic and operational risks across the council considering our risk appetite,
- Establishing clear roles, responsibilities and reporting lines for risk management across the council,
- Incorporating the assessment of risk into all key decision making and planning processes of the council,
- Using SPAR.net for recording, assessment, monitoring of controls and reporting of risks.

3 Terms explained

3.1 Risk Management

3.1.1 Risk can be defined as the effect of uncertainty on objectives, whether positive or negative.

3.1.2 Risks, therefore, need to be managed to successfully deliver the council's objectives. Risks should be fully understood and their probability (likelihood) and consequences (impact) subsequently managed.

3.2 Risk Matrix

3.2.1 A risk matrix is used in the risk assessment process. It creates a risk score from the combination of the likelihood and the impact of the risk. The risk becomes more severe as the likelihood and impact increase.

3.3 Strategic Risk

3.3.1 A strategic risk is generally managed by a Director or Assistant Director. It is something with the potential to cause harm (including ill health/injury; damage to assets; loss of reputation; environmental pollution; financial losses; increased liabilities etc). It can be an event or series of events that may impact on the delivery of the council plan and other major projects.

3.4 Operational Risk

3.4.1 Operational risks are managed by Director or Assistant Director and managers and are defined as risks that can affect the delivery of individual services but would not, in isolation, threaten our overall objectives.

3.5 Project Risk

3.5.1 Project risks are managed by the Project Manager (aligned to the Council's Project Management Framework) and are defined as risks that can affect the delivery of the defined project outcomes.

3.6 Pure Risk

3.6.1 This is the risk in its raw state without any mitigating controls (control actions in SPAR.net) in place.

3.7   Residual Risk

3.7.1   A residual risk is the remaining potential for harm to persons, property or the environment following all possible efforts to reduce predictable hazards. In other words, it is the risk that remains after a risk assessment has been carried out and control actions have been put in place. This risk needs to be monitored to keep the control actions up to date.
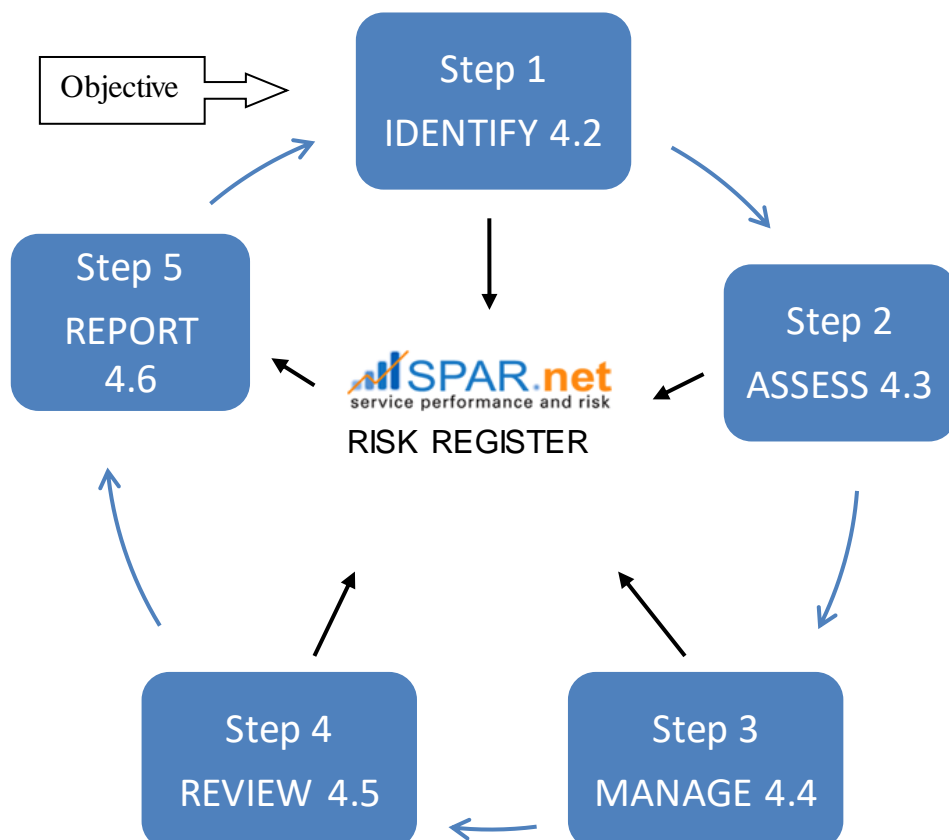
4   What is the council's policy?

Risk Management Guidance

4.1   Process Model

The process followed by us to manage risk is shown in the diagram below (see fig 4.1) and described in detail in the following paragraphs.

Fig 4.1

4.2   Step 1 - How and when to Identify Risk

4.2.1 The majority of risks are identified at the annual service planning days where barriers to specific business objectives can easily be recognised. All staff have a duty to report emerging risks to their Director or Assistant Director at anytime. Risks can raise and be identified when the following events occur:

- Internal or external processes change
- Staff/members leave and or restructuring takes place
- Partners change or restructure
- Legislation is revised or introduced
- The social and or economic climate alters
- An incident occurs (too late!)

4.2.2 To help in the risk identification process a range of the most common risk assessment techniques are set out in the table below (Table 4.2.2). These can be used as part of the service planning process or when an event as outlined above occurs.

Table 4.2.2

Techniques	Description
• Questionnaires and checklists	Individually designed questionnaires and checklists to collect information to assist with the recognition of the significant risks.
• Workshops and brainstorming	Collection and sharing of ideas and discussion around the events that could impact on the objectives
• Audit and inspection reports	To understand and check that processes and procedures are in place and working
• Flowcharts and dependency analysis	Analysis of processes and operations with the organisation to identify critical components that are key to success
• SWOT and PESTLE analyses	Strengths weaknesses opportunities threats (SWOT) and political economic social technological legal environmental (PESTLE) analyses offer structured approaches to risk recognition

4.2.3 The following are areas of risk which **have** to be assessed by Director or Assistant Director.

- Fraud, theft or corruption – including, falsification of records, misuse of resources (including computer hardware/ software) and a criminal act falling within the Fraud Act (e.g. false representation, failure to disclose information, abuse of position etc).

- Non- compliance with statutory requirements or legislation – including, unawareness of legislative requirements and ignoring legislative requirements

- Non- compliance with our policy or procedures – including, breaches to financial regulations or contract standing orders, non-compliance with council policies including the our code of conduct for staff and councilors and failure to follow manuals, procedures and guides

- Change management – including, new initiatives and/or new ways of working changes to existing policies or new policies

- Disclosure of sensitive information – including, our 'not for publication' matters made public, failure to dispose of confidential waste appropriately, external/ internal attack on computer hardware/ software and errors or omissions affecting externally published material

- Insufficient resources – including, absence or sickness, unfilled vacancies, deficient or lack or computer resources, insufficient funding, recruitment and retention difficulties

- Poor performance management – including, failure to measure or meet externally set performance targets, failure to meet internally set performance targets, failure to benchmark costs and performance and failure to set achievable goals and targets.

4.2.4 We have two categories of risk; strategic and operational (see 3.2 and 3.3 for definitions). There is a relationship between the two classes of risk which means that the cumulative effect of the unsuccessful management of operational risks will eventually represent a strategic risk, such as the failure of a number of key services or the significant loss of resources. We also have specific risks identified with projects which are standalone to that project (see 3.5 for defintion).

4.2.5 Expressing the risks as a statement is often harder than it first seems. It may require rethinking some basic assumptions about a situation and re-evaluating the elements that are most important. For example, "lack of staff" is not in itself the complete risk but a consequence of another action. Try to identify the root cause, ask, "why is there a lack of staff" and develop it into a risk that expresses how the issue will impact upon achievement of our strategic objectives.

4.2.6 When writing a risk description, try to include these three parts: event – consequence – impact. This will ensure that the focus, therefore the action, is placed on the event:

1) An Event	2) A Consequence	3) The Impact
Loss of ….. Failure of ….. Failure to …. Lack of …. Inability to …. Inadequate ….. Delay in ….	….. leads to	…. resulting in

For example:

The **lack of** performance information, public consultation and forward planning, **leads to** a fragmented approach to service development and our ability to meet recycling targets might not be achieved**, resulting in** reputational damage to the Council.

4.3   Step 2 - How to Assess a Risk

4.3.1   Not all risks can be eliminated completely, but the likelihood and impact can be reduced or better controlled through assessment, control actions, monitoring and review.

4.3.2   Strategic or operational risks should be assessed in the context of the scale of risk associated with each. This may be determined by considering:
- Likelihood of the risk occurring
- Impact, or severity of the consequences should it occur

4.3.3   Risks are assessed by selecting a scale for both likelihood and impact and multiplying them to produce a risk rating. This rating then falls within one of the following categories in the matrix: high, medium or low.

4.3.4   Once a risk has been identified the first step in the assessment process is to work out the pure risk status (see 3.4) this is achieved by determining the likelihood of the risk occurring by selecting the appropriate score from table below (table 4.2.1).

Table 4.2.1

LIKELIHOOD - GUIDE TO ASSESSMENT				
Likelihood of Occurrence	Score	Chance	Description	Indicators
Very Likely	4	>75%	Almost certain to happen within six months	Happens frequently and/or encountered on a daily, weekly or monthly basis or will happen within 6 months.
Likely	3	40-75%	Will probably happen within 12 months	Happens occasionally, expected to occur at some point over the next 12 months
Unlikely	2	10-40%	Possible – may happen. Not expected between 1 - 3 years	Not expected to happen in the next 1 - 3 years
Remote	1	Less than 10%	Rare – do not believe this will happen except in exceptional circumstances. Not expected between 3 – 10 years.	Has happened rarely in the past or never before

4.3.5   Next assess the impact that the occurrence of the risk would have on the corporate objective, the delivery of the service, or objectives of the project if it should occur. Do this by selecting the appropriate score from table below (table 4.2.2).

Table 4.2.2

Financial loss and/or outcomes with financial implications	Failure to provide statutory duties / meet legal obligations	Reputation	Service Disruption (days)	Performance	Health & Safety
SCORE 4	**MAJOR - IMPACT / OUTCOME** (One or a combination of the following)				
Errors or omissions affecting relevant separate budgets >25k or > 75% of budget, (whichever the smaller) Loss of external grants and funding in > £25k	Litigation / Claims / Fines Directorate > £125k Corporate > £250k	Adverse national media interest leading to : Officer(s) and / or member(s) forced to resign Failure to attract or retain suitable partners or suppliers	Service disruption of over 3 days	Failure to provide an excellent level of customer service Failure to identify external opportunities and threats Failure to learn from mistakes that have council wide implications	Death of an individual or several people Permanent disability caused to an individual or several people
SCORE 3	**SERIOUS - IMPACT / OUTCOME** (One or a combination of the following)				
Errors or omissions affecting relevant separate budgets from £10k - £25k or 50-75% budget (whichever the smaller) Loss of external grants and funding from £10k - £25k	Litigation / Claims / Fines Directorate £25k - £125k Corporate £50k - £250k	Adverse local or regional media interest leading to : Public embarrassment for Council Members or staff Recruitment and retention difficulties affecting one service due to low staff morale	Service disruption of between 2-3 days	Failure to provide an adequate level of customer service Failure to identify internal opportunities and threats affecting the whole council Failure to learn from mistakes that have directorate wide implications	Major injury to an individual or several people
SCORE 2	**SIGNIFICANT - IMPACT / OUTCOME** (One or a combination of the following)				
Errors or omissions affecting relevant separate budgets from £1k - £10k or 25 – 50% of budget (whichever the smaller) Loss of external grants and funding from £1k - £10k	Litigation / Claims / Fines Departmental £1k- £25k Corporate £10k - £50k	Contained within the Council (Questions raised by members) Embarrassment for council Members or staff, not public Some impact on staff morale in more than one service with no effect on recruitment or retention	Service disruption of between 1-2 days	Failure to identify and utilise staff potential within individual services Failure to identify system inefficiencies and bottlenecks Failure to learn from mistakes that have service wide implications	Minor injury to an individual or several people

SCORE 1		MINOR - IMPACT / OUTCOME (One or a combination of the following)			
Errors or omissions affecting relevant separate budgets up to £1k or 25% of budget (whichever the smaller) Loss of external grants and funding up to £1k	Litigation / Claims / Fines Departmental < £1k Corporate < £10k Scrutiny by regulatory body	Contained within the Service (Letters from the public) Some impact on staff morale in one service with no effect on recruitment or retention	Service disruption of less than 1 day	Failure to learn from mistakes that have implications for individual members of staff	Discomfort caused to an individual or several people

4.3.6 The likelihood and impact scores then need to be multiplied together to give the 'pure risk' score using the risk matrix below (fig 4.2.2).

Fig 4.2.2

Impact	4 Major	4	8	12	16
	3 Serious	3	9	9	12
	2 Significant	2	4	6	8
	1 Minor	1	2	3	4
		1 Remote	2 Unlikely	3 Likely	4 Very Likely
		Likelihood			

4.4 Step 3 - Manage the residual risk

4.4.1 Having identified a risk and assessed its impact and probability, the next step in the process is to develop actions to manage the risk. These are referred to as control actions. Controls are intended to help in mitigating either the impact or likelihood of the risk.

An example of a control action follows:

Risk Title
- **Failure to adequately anticipate or respond to a major health or environmental incident**

Example of a control action to mitigate the risk
- **Effective local plan for emergencies - The Emergency Planning Officer has drawn up emergency plans for key council personnel**

4.4.2 It maybe that a risk will need more that one control action and in more complex issues where, for example, the risk of inadequate ICT resilience is identified, the controls needed are both more sophisticated and numerous, and will be part of a whole array of measures that need to be taken.

4.4.3 In light of the control actions that have been put in place the risk now needs to be re-assess to find the level of **'residual risk'**(see 3.5 for definition). As in step 1 using the likelihood and impact tables (tables 4.2.1 and 4.2.4) determine the likelihood and impact of the risk with the controls in place. Again multiply those scores together and using the risk matrix (fig 4.2.4) identify the residual risk score.

4.4.4 Consider the action to be taken after determining the residual risk (see table 4.2.3 below).

Table 4.2.3

ACTION TO BE TAKEN AFTER DETERMINING RESIDUAL RISK		
12 - 16	High	Immediate action required
6 - 9	Medium	Evaluate effectiveness of current controls and actions and implement any improvements necessary before next review period
1 - 4	Low	Limited action, incorporate into current plans

4.4.5 Determine whether there are any opportunities within the risk assessment process.

4.4.6 Determine who will ultimately be responsible for the risk. This roll will involve monitoring the control actions and writing the reviews on the SPAR system. This person is called the responsible officer.

4.4.7 Enter the risk information into SPAR.net the corporate risk register database that records details and ownership of identified risks and their associated control actions. Refer to the SPAR Risk Guidance and/or the Management Information Officer for help with data entry.

Note: Access to and training on the use of SPAR.net is available from the Management Information Officer

4.5   Step 4 - Review the residual risk

4.5.1 Responsible officers should review their risks (including updating the SPAR system) according to their unmitigated risk score. A guide to the recommended frequency of reviews can be seen below:

Unmitigated Risk Score (pure status)	Review Interval

16	Monthly
12	Quarterly
6-9	Twice a year
1-5	Twice a year

4.5.2   Operational risks should be monitored regularly as part of the performance management within all services. This includes assessing whether the control actions are still adequate or need revising and or replacing. SPAR.net should be updated with any changes as soon as they arise.

Note: All risks have the ability to increase in severity very quickly, so if the risk does look more likely to happen do not wait until the next review is due … do something about it now.

4.6   Step 5 - Reporting risks

4.6.1   All risks will be reported to the Audit and Governance Committee at least on a bi-annual basis. These reports will have been seen by SLT prior to each committee meeting. As part of improved performance management reports will also be taken into Cabinet from 2024/25.

4.6.2   The Management Information Officer will inform all responsible officers of the reporting deadlines and send reminders about updating the SPAR system.

4.6.3   A member of the Audit and Governance Committee will act as a risk representative on behalf of the Committee. This member will familiarise themselves with the risk register and meet with the Management Information Officer as required.

4.7 Training

Risk management training is provided specifically for managers and officers who are responsible for maintaining the risk register. Training will also be provided to Audit & Governance and Cabinet Members.

4.8 Outcomes

By following this policy our management of risks should be fully embedded into the culture of the organisation. It should be possible to identify, assess, review and report risks in a uniform and structured way.

This framework will help protect the council from liabilities which might prevent us from carrying out our day-to-day activities.

4.9 Who is responsible for delivery?

The following list describes what each group or person is responsible for:

Audit & Governance Committee

- To formally approve the Risk Management Policy and Guidance.
- To monitor our risks and keep under review our risk action plans.

Senior Leadership Team
- To ensure risk is managed effectively and in accordance with the Risk Management Policy and Guidance.
- Responsible for the setting of the Councils risk appetite and tolerence levels and making decisions with proper consideration of risks
- To report to the Audit and Governance Committee as necessary.

Section 151 Officer
- To develop the Risk Management Policy and Guidance.
- To organise appropriate training for members and employees.
- To support the council in the effective development and implementation of the risk management framework and process including ensuring the process is embedded at all levels.
- To report to SLT at least bi-annually the risk register.

Directors and Assistant Directors
- To identify and assess operational risks and ensure that they are entered onto the SPAR.net system.
- To manage, review and report on (or delegate the management, review and reporting of) risks effectively in their service areas.

Senior Risk Owners
- Enter new risks on the SPAR.net system if not entered by the Directors or Assistant Directors including those identified by SWAP during service area audits.
- Monitor risks that they are responsible for i.e. ensure control actions are up-to-date.
- Work to deadlines for updating SPAR.net when risk reviews are required.

Member Risk Representative (from the Audit and Governance Committee)
- To liaise with Management Information Officer regarding the status of the risk register.
- To lead on risk management on behalf of the Audit & Governance Committee

Management Information Officer
- To liaise with Member Risk Representative and Section 151 Officer regarding the status of the Risk Register.
- To ensure responsible officers know the deadlines for updating SPAR.net.
- To send emails to responsible officers to remind them to update the SPAR.net system.
- Collate and produce at least bi-annual reports for SLT and the Audit and Governance Committee. Plus produce any other reports required.
- Council's advisor on all aspects of risk management and the implementation of risk management.
- Preparation of risk management reports.
- Provision of risk management training.

Managers and other employees
- To manage risk effectively in their job and report risks to their Managers or Strategic Leads.
- To comply with Risk Management Policy and Guidance.

SWAP
- To carry out audits of the Risk Register in order to keep everything on track.
- To review risk within specific Service Area Audits.

5   Equality impact considerations – the policy is high relevance to equality if it has a big impact on residents and users of the service

Low

The Risk Policy is low impact however the outcome of some of our risks could have a high impact on local residents. Therefore, equality should be considered when all risks are assessed and reviewed.

6   Appendices and other relevant information

Click here to enter appendicies and other information

7   Who authorised the policy/strategy and date of authorisation.

Audit and Governance Committee date

8   Related Policies/Strategies, Procedures and Legislation

SPAR.net Risk Guidance Document. The Policy is integrated to other documents of the Council such as Coporate Governance Famework, Financial Plan, Business Continutiy plans etc.

9   Policy date for review and responsible officer

Date for next review February 2028 by Director of Finance