

# Risk Management Policy 2026/27



## 1.0 Background

1.1 The Risk Management Policy details Mid Devon District Council's (MDDC) framework for managing risk. Risk Management is an integral part of the Council's Corporate Governance arrangements and there is a statutory responsibility under the Account and Audit Regulations (2015) to put in place risk management arrangements.

1.2 The Association of Local Authority Risk Managers defines Risk Management as:

*“Risk Management is the culture, processes and structures that are directed towards effective management of potential opportunities and threats to the organisation achieving its objectives”.*

1.3 Maintaining, developing and improving public services in the current financial climate requires opportunities to be taken whilst managing the risks involved. Therefore Mid Devon District Council's definition of Risk Management is:

*“The planned and systematic approach to identify, evaluate and manage the risks to, and opportunities for, the achievement of objectives”*

## 2.0 Purpose, Aims and Objectives

2.1 The purpose of the Policy is to embed Risk Management in MDDC by establishing a risk management framework, which provides:

- An efficient control environment
- Accountability for risk management throughout the organisation
- A culture where officers and Members are able to be more creative and innovative in taking opportunities that benefit the Council and the District provided that there is clear analysis of the risks and a robust justification for the decision
- A well-established risk assessment process which ensures that risks are considered and managed as part of the decision making process
- Performance monitoring of risk management activity
- Communications process to support risk management
- A robust opinion for the Annual Governance Statement which comments of the adequacy of the Council's risk management arrangements

2.2 The aim of the MDDC Risk Management Policy is to adopt industry standard practices in the identification, analysis, evaluation and treatment of risks and opportunities.

2.3 It is acknowledged that some risks will always exist and will never be eliminated. All employees must understand the nature of risk and accept responsibility for risks associated with their area of authority. The necessary support, assistance and commitment of senior management will be provided.

2.4 The risk management objectives of MDDC are to:

- Embed risk management into the culture of the council
- Fully incorporate risk management as an integral part of corporate planning, business planning, project management and performance management
- Manage risk in accordance with best practice and in particular in accordance with the requirements of the Annual Governance Statement
- Consider legal compliance as a minimum
- Prevent injury and damage and reduce the cost of risk
- Raise awareness of the need for risk management

2.5 These objectives will be achieved by:

- Establishing a clear risk management process that is communicated to all officers and Members
- Clearly defined roles and responsibilities for risk management
- Providing risk management training to officers and Members
- Completing corporate and service risk management workshops as required to identify risks
- Maintaining and reviewing corporate and service risk registers, with responsible officers assigned to each risk
- Ensuring that committee reports include an assessment of associated risks
- Identifying risks and opportunities in relation to working in partnerships
- Ensuring that the Cabinet and Audit Committee receive regular reports on strategic risk and the actions taken to manage these.

2.6 The following sections consider how the Council will implement the above objectives.

### 3.0 Roles and Responsibilities

3.1 The following groups and individuals have the following roles and responsibilities for risk management at MDDC.

3.2 The **Audit Committee** will approve this Risk Management Policy and any subsequent revisions. They will also receive and scrutinise quarterly reports on the Council's Corporate Risk Register, the actions taken to manage these risks, and will consider the adequacy of the Council's risk management arrangements as part of the Annual Governance Statement.

3.3 The **Leadership Team** is primarily responsible for setting the organisation's risk appetite and identifying corporate risks, as well as being responsible for determining mitigating actions and delegating responsibility for the control of the risks. The wider management will also be responsible for monitoring the progress of managing risks and will review committee reports.

3.4 The **Cabinet** will monitor the effective implementation of risk management at MDDC by receiving quarterly reports on the Council's corporate risks.

3.5 The **Policy Development Groups (PDGs)** will receive updates on risks relating to any policy development matters as required. Any concerns or issues will be reported to the Cabinet.

- 3.6 The **Leader of the Council** will communicate the importance of risk management to other Members. They will also act as a sounding board and provide “critical friend” challenge to the risk management process.
- 3.7 **Directors/ Heads of Service** will:
- Lead the risk management process within their services and ensure that business plans include an annual assessment of risk
  - Identify and manage significant operational risks by carrying out risk assessments with their teams as and when this becomes appropriate e.g. if making a significant change to service or undertaking a project
  - Develop actions to mitigate the risks identified, assigning responsibility for implementing controls and setting target dates for implementation
  - Ensure that all corporate and service risks are managed on SPAR (the Council’s corporate performance and risk management system) and other service risk assessments held on the corporate health and safety drive.
  - Regularly review risks associated with their service area(s) ensuring that the agreed actions and deadlines have been met
  - Ensure that any briefing papers/ reports that they produce to make changes to their services effectively consider associated risk implications.
- 3.8 The **Corporate Performance and Improvement Manager** is responsible for providing assurance to the Council through monitoring the implementation and effectiveness of this Risk Management Policy. They will also comment upon the effectiveness of the risk management process in work undertaken to support the Annual Governance Statement. They will coordinate the corporate risk management process and provide reports to Audit committee and to Cabinet.
- 3.9 **Internal Audit** will consider risk and controls in their audit reviews and report on the adequacy of risk management in those areas. Internal Audit will also undertake audits of the Risk Management policy/ control framework.
- 3.10 The **Health and Safety Committee** is responsible for reviewing the measures taken to ensure the health and safety of all those who work in and visit the council or may be affected by its activities - ensuring that people are not exposed to risks and that the risks are mitigated effectively. Where concerns are raised these will be escalated to the Health and Safety Officer and Leadership Team for action.
- 3.11 All **employees** need to have an awareness of risk management and are responsible for ensuring that they manage risk effectively in their jobs and report hazards and risks to their line manager.
- 4.0 Strategic, Operational and Project Risks**
- 4.1 Broadly speaking risks can be divided into three categories:
- **Strategic** – risks which need to be taken into account in judgements about the medium to long term goals and objectives of the Council whilst at the same time considering the opportunities
  - **Operational** – risks and opportunities which managers will encounter in the daily course of their work

- **Project** - risks and opportunities which will be encountered during specific tasks/ projects

## 4.2 Strategic Risks

4.2.1 The management of strategic risks is a core responsibility of the Leadership Team and the Corporate Management Team. The identification and management of strategic risk should be factored into corporate and service planning.

4.2.2 The Leadership Team are primarily responsible for the management of corporate risks (strategic risks which could impact on the achievement of corporate priorities).

4.2.3 The Corporate Management Team are primarily responsible for the management of service risks (strategic risks which could impact on the achievement of service priorities).

4.2.4 The major categories of strategic risk are:

- **Political** – associated with failure to deliver either local or central government policy. The council could also potentially be at risk from the actions of other agencies, other councils, partner organisations, etc.
- **Economic** – affecting the ability of the council to meet its financial commitments. These include internal budgetary pressures as well as external factors affecting the economy as a whole.
- **Social** – relating to the effects of changes in demographic, residential or socio-economic trends on the council's ability to deliver its objectives.
- **Technological** – associated with the capacity of the council to deal with the pace/ scale of technological change, or its ability to use technology to address changing demands.
- **Legislative** – associated with current or potential changes in national or European Law.
- **Data Protection/ Information Security** – this includes the consequences of data/information transfer between the Council and other Bodies e.g. Government Connect, Partnership working, etc.
- **Environmental** – relating to the environmental consequences of progressing the council's strategic objectives (e.g. in terms of climate change including energy efficiency, pollution, recycling, landfill requirements, emissions, etc.).
- **Health and Safety** – This includes all aspects of Health & Safety as well as the Corporate Manslaughter legislation
- **Competitive** – affecting the competitiveness of the service (in terms of cost or quality) and/ or its ability to deliver Value for Money.
- **Customer/ Citizen** – associated with failure to meet the current and changing needs and expectations of customers and citizens.
- **Partnership** – associated with working in partnership or sharing services with another local authority or partner

## 4.3 Operational Risks

4.3.1 Operational risks are those which managers and staff will encounter in the daily course of their work. These may be:

- **Professional** – associated with the particular nature of each profession (e.g. housing service concerns regarding the welfare of tenants).

- ❑ **Financial** – associated with financial planning and control and the adequacy of insurance cover.
- ❑ **Legal** – related to possible breaches of legislation.
- ❑ **Personal Safety** – related to lone working and the potential to encounter aggressive or confrontational people whilst carrying out their duties.
- ❑ **Physical** – related to fire, security, accident prevention and health and safety (e.g. hazards/risk associated with buildings, vehicles, plant and equipment, etc).
- ❑ **Contractual** – associated with the failure of contractors to deliver services or products to the agreed cost and specification.
- ❑ **Technological** – relating to reliance on operational equipment and the potential for technological failure (e.g. IT systems or equipment and machinery)

#### 4.4 **Project Risks**

4.4.1 Risks which will be encountered during specific tasks/ projects being undertaken. These may be:

- ❑ **People** – associated with whether we have the right people with the right skills involved in the project. This also concerns getting buy in from staff at all levels of the organisation, Members and potentially external stakeholders
- ❑ **Technical** – Connected to technology including, but not limited to software, hardware, digital network, digital assets, system security, and new and changing technology and changing regulatory requirements.
- ❑ **Cost** – associated with the potential for the project to go over budget if the people and technical matters are not delivered as per the Business Case and Project Initiation Document.
- ❑ **Time** – ensure that the right amount of time is allocated to the project as well as sufficient contingency as slippage can cause to project delay/ failure and this can also have an impact on cost and quality
- ❑ **Quality** – depending on what goes into the project will determine the quality of the output

#### 4.5 **Opportunities**

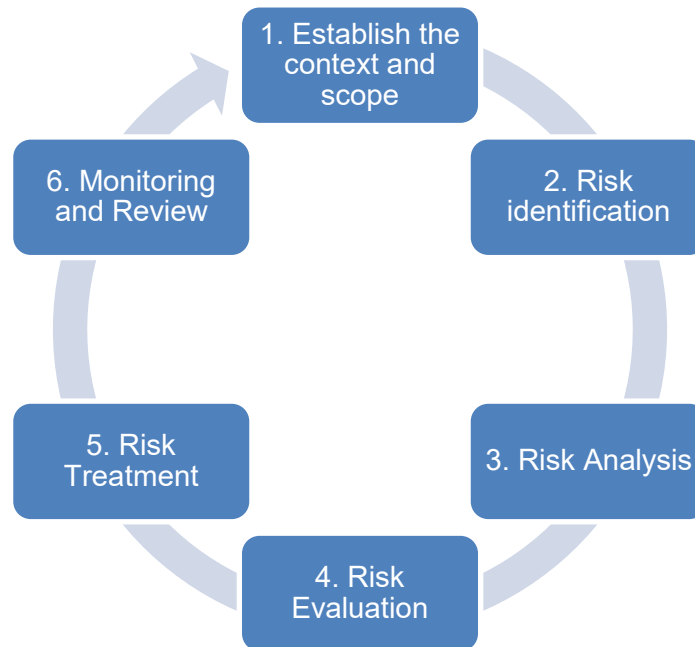
4.5.1 Opportunities are to be considered at the same time as risk. Examples may include:

- ❑ Spend to save projects where the Council will benefit from reduced expenditure or increased income in the future
- ❑ Transformational change which will generate cost savings or an income stream
- ❑ Opportunities for partnership working with our stakeholders or other local authorities
- ❑ Opportunities to streamline working processes
- ❑ Opportunities to boost the local economy
- ❑ Opportunities to deliver and improve housing within the District
- ❑ Opportunities to protect and enhance our environment
- ❑ Opportunities to make a difference to our communities and to empower them
- ❑ Delivery of the objectives in the Corporate Plan and Service Business Plans

4.6 The categories are neither prescriptive nor exhaustive. However, they should provide a framework for identifying and categorising a broad range of risks and opportunities for the Council as a whole, as well as service areas.

## 5.0 RISK MANAGEMENT PROCESS

5.1 Risk management can be defined as a six step process. Steps 2 to 4 are collectively known as a strategic risk assessment.



Underpinning each of these stages is communication and consultation with interested parties. The aim of this is to ensure internal and external (if appropriate) stakeholders are considered and involved in our work to understand and define our risks.

### 5.2 Step 1: Establish the Context and Scope

Risk management happens at different levels (e.g. strategic, operational, project), for different purposes, and at different times. When working on risk management it is important that everyone involved understands the scope of the work they are undertaking. Three questions should be considered:

1. What are we considering risks to?  
*For example, if the goal is to produce a project risk register, participants should be identifying risks to the project's objectives.*
2. What timescales should be considered?  
*Normally this would tie in with a planning cycle, or a project lifetime.*
3. Who needs to be involved at each stage and what information do they need?

Ideally the same group will be involved throughout the risk assessment stages (steps 2-4) to provide a consistent approach.

### 5.3 Step 2: Risk Identification

Once the context and scope of the risk management activity has been established, risks can be identified. This should be a group activity, pooling all relevant expertise. It can be done in a number of ways, including:

- Brainstorming session or workshop
- Interviews
- Meetings with small groups of people
- Questionnaires
- Taking from other Council strategies
- By consulting other risk or compliance type services, e.g. Health & Safety, Information Security, Internal Audit etc.

Existing sources of information can also be used to help identify potential risks. To help identify risks, it can be helpful to think about the different sorts of risks that might arise (as detailed at Sections 4.2.4; 4.3.1; and 4.4.1).

As risks are identified, it is crucial for them to be clearly defined. Failure to do so can cause confusion later about the exact nature and/or consequence of the risk. This can lead to ineffective controls being implemented, or the risk analysis being over or underestimated. Risks should be defined in terms of the potential cause(s) and consequence(s).

### 5.4 Step 3: Risk Analysis

The purpose of this stage is to get a better understanding of each risk. The analysis also helps prioritise which risks are most significant and need more attention, effort, and resources. It also allows comparison between different types of risk using a risk matrix that plots likelihood and severity.

Each risk will be analysed for the likelihood it will happen (scored from 1 to 5) and the severity (scored from 1 to 5) if it did happen.

Below is a brief guide to scoring risks. The examples below are neither prescriptive nor exhaustive. Fuller guidance is provided to officers in associated guidance.

#### Risk Severity

##### 1 – Very Low

- Localised minor injury or health impact to one person (no time off work required)

##### 2 - Low

- Localised minor injury or health impact to one person (small time off work required e.g. less than 1 week)
- Small financial loss or service cost increase (less than £5,000)

##### 3 - Medium

- Minor injury or health impact to multiple persons (small time off work required e.g. less than 1 week)
- Injury or health impact to one person (substantial time off work required e.g. more than 1 week)
- Financial loss or service cost increase (e.g. over £5,000)
- Theft of Council property, assets, resources (less than £5,000)
- General loss of confidence and trust in the Council within the local community

#### 4 - High

- Serious injury or health impact to one person
- Loss of contract, resource, data or equipment resulting in long-term inability to maintain service or short-term inability to maintain several services
- Localised damage to Council property / premises
- Localised environmental impact

#### 5 - Very High

- Serious injury or health impact to several or death of a person
- Loss of contract, resource, data or equipment resulting in long-term inability to maintain several services
- Serious damage / destruction of Council property / premises
- Prosecution for failing to comply with / serious breach in, or non-application of legislation / accepted standards
- Serious, District-wide environmental impact
- Serious financial loss or service cost increase (e.g. over £100,000)

### Risk Likelihood

#### 1 - Very Low

- Substantive, effective, tested and verifiable internal controls / mitigating actions in place
- Previous experience at this and other similar organisations makes this outcome highly unlikely to occur

#### 2 - Low

- Effective internal controls / mitigating actions in place
- Previous experience discounts this risk as being likely to occur but other organisations have experienced problems in this area

#### 3 - Medium

- Some internal controls / mitigating actions in place, but in need of review / improvement
- Existing controls generally work but there have been occasions when they have failed and problems have arisen
- The Council has in the past experienced problems in this area but not in the last 12 months

#### 4 - High



- Poor or ineffective internal controls / mitigating actions in place, or existing controls are generally ignored
- The Council has experienced problems in this area within the last 12 months

#### 5 - Very High

- No internal controls / mitigating actions in place
- The Council is experiencing problems in this area or expects to within the next 12 months

This assessment should be made considering controls that are already in place and working effectively. Controls that are not yet in place should not be considered.

The impact should be considered against the relevant objectives, e.g. corporate risks against corporate objectives, project risks against project objectives. The risks should then be plotted on the risk matrix once all likelihood and severity scores have been agreed.

 <b>Risk Severity</b>	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
	<b>Risk Likelihood</b> 					

The overall risk rating for a risk is calculated by multiplying the risk severity and the risk likelihood, this is shown on the risk matrix.

The risks will then need to be considered in conjunction with any opportunities when making decisions (or taking risks).

### Benefits of Opportunities

The assessment methods for determining the potential benefits of opportunities can include:



- Assessing the increased income/ reduced expenditure from the innovation
- Quantifying the number of potential new customers
- Calculating the potential sales growth that could stem from capturing the opportunity
- Calculating the return on investment for a particular project and whether that is the level of return that the Council is looking for
- Considering the value added as a result of capitalising on the innovation e.g. the benefit to the community

### 5.5 Step 4: Risk Evaluation

The evaluation step is the final stage of the risk assessment process. This will inform decisions about the treatment of the risk. The first stage is to identify what the appetite for risk is. The council's current risk appetite is that:

- Risks with a risk rating between 15 and 25 are classed as high risk (red);
- Risks scoring between 5 and 12 are classed as medium risk (amber); and
- Risks scoring between 1 and 4 are low risk (green).

Any risk which scores 10 or above is deemed above the risk appetite and treatment is required. Risks which score between 5 and 9 may require treatment at discretion of the risk owner(s). Treatment is particularly likely where it is a strategic risk.

 Risk Severity	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
	1	2	3	4	5	
	Risk Likelihood 					

The final stage of the risk evaluation will include a decision about how to manage each risk:

1. Do nothing: No further treatment of the risk is required other than to monitor the risk and ensure any controls continue to be effective (Below the risk appetite).
2. Treatment: Further treatment is required (Above the risk appetite).
3. Further Analysis: More analysis of the risk is required before it can be fully evaluated.

When evaluating risks, the following should also be considered:

- The council as a whole has a zero tolerance approach to fraud. Fraud risks must be considered as part of the development of all risk registers
- The council will not tolerate any risks which could result in the breaking of any laws or regulations, or ultra vires (acting without its legal powers or authority)
- The response to any risk should comply with relevant council policies and procedures
- The level of confidence of the risk is fully understood, i.e. the root causes, the potential consequences and the likelihood of it happening

## 5.5 Step 5: Risk Treatment

For risks which require management, appropriate treatment needs to be implemented. There are four options which should be considered:

1. Avoid the risk – By ending the activity, the Council's involvement in a project or partnership, or by doing things in a different way
2. Transfer the risk – By passing some or all of the responsibility for negative consequences to a third party, such as an insurer or contractor.
3. Take the risk – pursue the opportunity
4. Change the risk – by taking actions to reduce the likelihood or impact of the risk

The treatment approach will need to consider the current risk rating, a target risk rating (usually below the risk appetite line), and how quickly the Council wants to treat the risk.

In the risk treatment stage, a decision should also be taken as to whether the risk should be escalated, for example from a service level to a corporate level.

Factors affecting this decision include:

- The impact, should the risk occur, on other services within the Council
- Whether the risk requires coordinated action or higher level leadership to manage it

## 5.6 Step 6: Monitoring and Review

Each council service, project manager, or contract manager is responsible for maintaining a risk register as deemed necessary. A risk register is a list of all the related risks being monitored and managed.

The Corporate Risk Register will be coordinated by the Corporate Performance and Improvement Manager. Leadership Team will determine which risks are managed through the Corporate Risk process. The Corporate Risk Register will be reported quarterly to the Audit committee and to Cabinet.

Monitoring and review of risks should occur at least annually, but will likely require more regular review. The frequency should be determined by the group managing the risk, or the responsible project manager. It will be influenced by the types of risk, and their potential impact and likelihood.

Committee reports may also trigger a review of risks, and decision makers may wish to be made aware of how any decision may affect risks that have already been identified.

For each risk on a risk register the following information should be captured:

- Risk name and risk description
- Risk owner (who has ultimate responsibility for managing the risk)
- Current risk rating
- Risk actions (being taken to mitigate the risk), along with the responsible officer
- Any additional information as required to help with monitoring the risk.

Leadership Team and Members expect to see up to date and relevant review notes for the mitigating actions on all risks reported to Committee.

## **6.0 Risk Management Training, Guidance and Awareness**

6.1 For the benefits of Risk Management to be realised, it is necessary for the process to be embedded in the culture and operations of the organisation.

6.2 Strategic Risk Management training is available for officers. This will support officers to manage risk. Additional guidance and training will be developed for officers and Members as required.