South Downs National Park Authority


Risk Management Policy and Guidance 2019-2023

Version 0.1

Review Date	October 2023
Responsibility	Head of Governance and Support Services
Last updated	
Date approved	September 2019
Approved by	Policy and Resources Committee

1. Introduction & Purpose

1.1   Risk is an uncertain event or condition that, if it occurs, has an effect on at least one objective/outcome.

1.2   Managing risks is an iterative process and assists the Authority in making informed choices. It forms a key part of the organisations leadership and governance, and is fundamental to how the organisation is managed.

1.3   Risk can come from any number of sources such including:
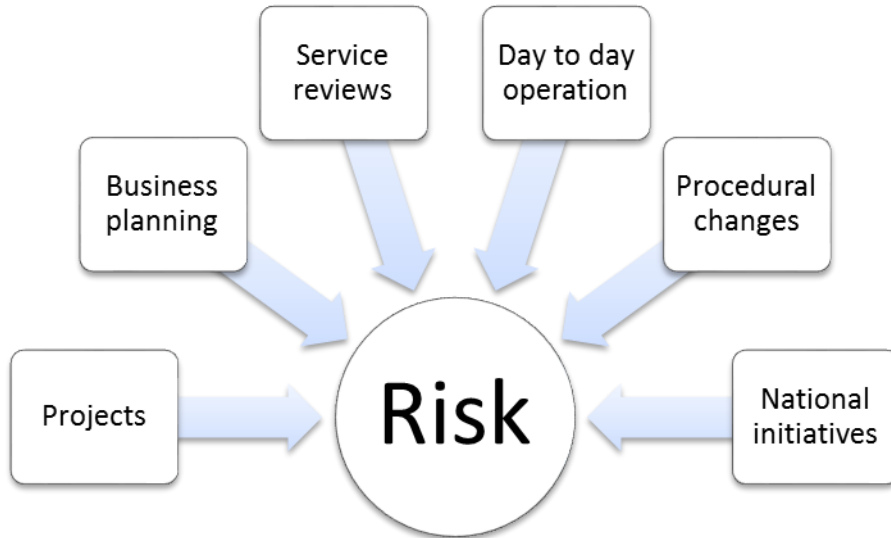
1.4   Risk management is the culture, processes & structure which come together to optimise the management of potential opportunities and adverse effects this is done by "the assessment of the probability of an event and its consequences". It also enables the effective use of resources, assists in securing the authority's assets and supports the authority's continued financial and organisational well-being. In order to deliver effective risk management the sdnpa will:

Foster a culture for risk management recognizing that effective managers make key decisions about risk and opportunities as an integral part of what they do on a daily basis;	**Integrate** risk management into existing processes as far as possible and not undervalue existing arrangements for dealing with risks;	Set a "**risk appetite**" – the level of risk the Authority is prepared to accept to inform planning, decision making and operations;
Make clear how to **escalate risks** if the "risk appetite" is exceeded, or has the potential to be exceeded;	Manage risks at the **lowest level** at which the manager has the authority, responsibility and resources to take actions;	Encourage **open and honest reporting** of risks and progress to manage risks;
Ensure a **consistent** approach;	Agree clear **roles and responsibilities** relating to the accountability, management , escalation and communication of key risks; and	**Improve** the effectiveness of the risk management arrangements and learn from experience.

1.5   The purpose of risk management is to safeguard an organisation, its customers and the interests of its stakeholders, by identifying and managing all threats to the achievement of its business objectives.

1.6   Risk Management considers the impact and likelihood of events, changes or issues affecting the achievement of objectives. The role of this policy and guidance is to support staff and Members in identifying, categorising mitigating and recording risk. It is not exhaustive and should be used as a starting point for risk management.

1.7   Further advice and the risk register template can be sought from the Head of Governance and Support Services if required. Information on risk management within projects is available from the Projects and Performance Team

2.   **Effective Risk Management**

2.1   Effective Risk management must be[1]:
- Integrated into all of the organisations activities
- Structured and comprehensive – producing consistent and comparable results
- Customised and proportionate to the needs of the organisation
- Dynamic and responsive to change
- Based on the best available information, both historic and current
- Must consider human and cultural factors
- Subject to review and improvement.

2.2   Risk Management needs to be proportionate to the level of risk in the organisation and the activities it undertakes. It should be aligned to existing corporate systems

---

[1] ISO 13000 second edition 2018-02

and needs to be practised at all levels across the Authority, including when it is working with others.

2.3   The Risk Management Policy and risk management procedures are in place to enable risks to be identified and managed at the most appropriate level. This relies on:
- an understanding of the principles of Risk Management;
- Risk Registers being completed and reviewed;
- escalation processes which involve reporting significant risks to more senior management levels; and
- clear roles and responsibilities – each team or project is responsible for ensuring that effective arrangements are in place for the identification of key risks.

3   Risk Registers

3.1   A Risk Register is a prioritised list of those risks which could affect the achievement of objectives. Risk Registers should cover all risk categories. The risk categories address issues/risks which may be external (those which are generally out of SDNPA control/influence and can affect our ability to deliver our strategies and policies) or internal issues/risks.

3.2   The value in creating a risk register is that it enables discussion about the risks facing the organisation. This will:
- foster an improved risk management culture;
- generate a better understanding of the problem;
- make sure sufficient resource is in place to deliver the defined mitigations; and
- lead to better decision making at the correct time.

3.3   The SDNPA has a Corporate Risk Register which:
- is developed by the senior managers across the organisation with emerging risks/mitigation added as appropriate;;
- is reviewed regularly
- prioritises risks, archives closed risks and reviews the direction of travel.

3.4   Directorate Management Teams will oversee risk registers relevant to their areas of delivery which are reviewed regularly and any significant risks escalated to the corporate risk register

3.5   Risk registers may also be developed for particular parts of the organisation and also for particular projects. Escalation from these registers will be to the Directorate risk register.

3.6   Risk Registers should set out:
- Reference number – unique number that does not change when the register is updated;
- Description of Risk;
- Inherent Likelihood – categorisation of the probability of the risk taking place without mitigations in place ;
- Inherent Impact – categorisation of the severity of the impact if the risk takes place without mitigations in place

- Mitigation – the measures the Authority is taking or has taken to reduce the change of the risk actually occurring or the consequences if it does;
- Residual Likelihood – categorisation of the probability of the risk taking place with mitigations in place ;
- Residual Impact – categorisation of the severity of the impact if the risk takes place; with mitigations in place
- Owner – who is responsible for monitoring this risk.

4   Risk Categories Checklist

4.1   Set out below are examples of types of risks that should be considered when identifying risks. These will not all apply to all situations, but you should consider if they apply to the issue being assessed. Any risks identified from the table below should be logged and the impact matrix (section 3, below) should be used to assess the potential impact of the risk.

4.2   As there may well be other examples under each category, these are intended as a prompt only

Professional/Managerial/Partnerships
- Recruitment/Retention of qualified staff   - Investing in Training   - Skill mix   - Over reliance on key officers   - Ability to implement change   - Management of partnership working
Economic/Financial
- Impact of national economic position   - Failure of major project(s)   - Missed business and service opportunities   - Failure to prioritize, allocate appropriate budgets and monitor   - Inefficient/ineffective processing of documents
Social
- Meeting the needs of disadvantaged communities   - Tracking the changes in population base   - Employment opportunities   - Regeneration   - Partnership working   - Life-long learning
Technological
- Functionality and reliability of IT systems - impact on service delivery   - Data Security issues/Information Governance   - Inability to implement change   - Obsolescence of technology   - Technology strategy
Legislative

- Meeting statutory duties/deadlines
- Breach of confidentiality/Data Protection Acts requirements/Information governance
- European Directives on Procurement of Services
- Implementation of legislative change

Contractual/Competitive

- Over reliance on key suppliers/contractors
- Ineffective contract management
- Contractor failure
- Lack of existing markets

Equalities

- Workforce Composition – across all persons who provide a service on behalf of the council and in its partnership work
- Appropriate recognition of the diversity of Service Users/Customers, e.g. age, ethnicity, gender, disability, religion
- Ensuring consistent minimum standards to meet legislative duties (incl. training, sharing policies & best practice)
- Altering working practices as necessary to meet diverse needs and ensure no discrimination
- Ability to demonstrate equalities in action (incl. methods to monitor, evaluate and review)

Political

- Impact of Strategic Priorities on business activities
- Clarity & cohesion in decision making
- Impact of Central Government policy on local policy/local initiatives

Environmental/Sustainability

- Sustainability/Climate Change
- Waste Disposal/Recycling Strategies
- Crime & Disorder Act implications
- Impact on quality of life in the Park
- Impact on transport network and other transport issues

Customer/Citizen

- Appropriate consultation
- Quality of customer care
- Access to services
- Views of Service Users
- Political support, e.g. Members

Fraud & Corruption

- Appropriate segregation of duties
- Security of Data
- Hospitality/Gifts Policy, Record Keeping and Monitoring
- Trends of working (e.g. unusual lone or late working) or sickness absence (potentially

fraudulent)
- Verification/Validation checks e.g. before staff/contractor appointments, cash transactions

5. Impact Matrix

5.1 Once a risk has been identified it is necessary to assess the likely impact of that risk, this can be done using this matrix. Each individual risk should be assessed on its own merits and the score noted, as this will form a key part of allocating a total risk score to each item.

Risk Score	Impact Descriptor	Impact Risk Scoring Guidance
1	Insignificant	**Impact on community life** insignificant disruption to community services, including transport services and infrastructure **Service Delivery** no service disruption, unlikely to cause complaint or instigate litigation **Economic** none/minimal financial burden (less than £100, can be resolved at local service / department level), minor interruption to income generation, no permanent loss **Environment** insignificant impact on environment **Reputation** organisation(s) reputation remains intact
2	Minor	**Impact on community life** minor localised disruption to community services or infrastructure less than 24 hours **Service Delivery** minor service disruption, complaint possible, litigation unlikely **Economic** minimal financial burden or disruption to income generation (less than £1,000 but greater than £100). Can be resolved at line manager/ service manager level through usual budgetary measures **Environment** minor impact on environment with no lasting effects **Reputation** minimal impact on organisation(s) reputation
3	Moderate	**Impact on community life** damage that is confined to a specific location, or to a number of locations, but requires additional resources. Localised disruption to infrastructure and community services **Service Delivery** moderate service disruption. High potential for complaints, litigation possible, but not certain **Economic** moderate financial burden (less than £10,000 but greater than £1,000). Interruption to income generation lasting less than 14 days, majority of income recoverable but at additional cost **Environment** limited impact on environment with short-term or long term effects **Reputation** moderate impact on organisation(s) reputation

4	Major	**Impact on community life** significant damage that impacts on and possible breakdown of some local community services. Requires support for local responders with external resources **Service Delivery** service closure for 1-7 days, complaints expected, litigation expected **Economic** major financial burden (less than £100,000 but greater than £10,000). Can include significant extra clean up and recovery costs. **Environment** significant impact on environment with medium to long term effects **Reputation** major impact on organisation (s) reputation / National adverse publicity
5	Catastrophic	**Impact on community life** extensive damage to properties and built environment in affected areas. General & widespread displacement of more than 500 people for prolonged duration. Community unable to function without significant support **Service Delivery** service closure for more than 7 days or closure of multiple services, complaints certain, litigation certain **Economic** catastrophic financial burden (greater than £100,000). Extensive clean up and recovery costs **Environment** serious long-term impact on environment and/or permanent change **Reputation** catastrophic impact on organisation(s) reputation. International adverse publicity

Likelihood

5.2 The likelihood of a risk occurring can be assessed using the table below. Each individual risk should be assessed on its own merits and the score noted, as this will form a key part of allocating a total risk score to each item.

Description	Likelihood of Occurrence
Almost Certain	The event is expected to occur in most circumstances.
Likely	There is a strong possibility the event will occur.
Possible	The event might occur at some time
Unlikely	Not expected, but a slight possibility
Rare	Highly unlikely. It could happen but probably never will

Risk Assessment

5.3 For Risk Assessment, it is necessary to show how the Risk Rating (Likelihood x Impact scores) was reached. This risk matrix should be used:

LIKELIHOOD	IMPACT				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Almost Certain (5)	5	10	15	20	25
Likely (4)	4	8	12	16	20
Possible (3)	3	6	9	12	15
Unlikely (2)	2	4	6	8	10
Almost Impossible (1)	1	2	3	4	5

5.4   Once the inherent risk has been scored in terms of likelihood and impact, it can be allocated priority for action to control/mitigate the risk. Mitigations should be put in place to impact either the severity or likelihood (or both) of the risk. Mitigations could include a change in the allocation of resources, communications, change s to processes or procedure etc. It is up to you to identify and put in place relevant mitigations to bring the risk level down to an acceptable level.

5.5   Residual Risk (i.e. that risk that remains after mitigations have been put in place) should be managed in line with the table below:

LIKELIHOOD	IMPACT				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Almost Certain (5)	5	10	15	20	25
Likely (4)	4	8	12	16	20
Possible (3)	3	6	9	12	15
Unlikely (2)	2	4	6	8	10
Almost Impossible (1)	1	2	3	4	5

Risk is considered minimal, no specific action required

Managed by manager/lead officer. Basic mechanisms to manage risk should be in place

Managed at Directorate Management Team level. Robust plans to mitigate and manage the risk should be in place. May be included on corporate risk Register

Managed at Directorate management team level and escalated to SMT for inclusion on corporate risk register. Robust plans to mitigate and manage risk should be in place

5.6   It will not always be possible to reduce the Risk Score to a lower risk rating, e.g. from a high score to low. This does not necessarily mean that it should stop the SDNPA undertaking the activity. The SDNPA has set out its appetite for risk across the various categories below. This risk appetite will help SMT and members in their decision making.

Escalation of risks

6.1   It is important that an aggregate picture of risk levels is available to ensure that the SDNPA has a comprehensive and accurate understanding of the level of risk to which it is exposed at any one time.

6.2   This requires the escalation of risks to the appropriate management level. The process to escalate a risk is that following assessment, the lead officer should refer any significant risk to a more senior management level.

6.3   A risk should be escalated to the management level above if mitigations cannot bring the residual risk level down to a manageable level in line with the table above.

Risk Appetite

7.1   The Authority's risk appetite is a statement of the level of risk it is willing to accept across the range of its activities. It enables the organisation to better communicate around issues of risk and assists members and SMT in their decision making roles, both formally and informally. When reviewing risk registers senior managers will be able to better assess if additional mitigations or actions are required to address risks. Equally, where the Authority is willing to accept a higher level of risk opportunities are not missed due to an overly cautious approach.

7.2   The SDNPA appetite for risk is set by members thorugh this policy and included in the regular risk register reporting to Policy and Resources Committee. The statement is set out below and is "scored" using the following critiera:

- **Averse** Avoidance of risk and uncertainty is a key organization objective.
- **Minimal** Preference for ultra-safe options that are low risk and only have a potential for limited reward.
- **Cautious** Preference for safe options that have a low degree of risk and may only have limited potential for reward.
- **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 risk, reward and value for money.
- **Hungry** Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk

Risk Category /appetite	Averse	Minimal	Cautious	Open	Hungry
Service Delivery (how we deliver our services)				X	
Economic/Financial (how we manage and allocate our resources)			X		
Reputation (how we are seen by customers, partners and the public)			X		
Health and Safety (of our staff and customers)		X			

The Authority seeks to operate within a limited overall risk range. The Authority's lowest risk appetite relates to safety including employee health and safety, with a higher risk appetite towards those activities directly connected with the Authority's Purposes and Duty. The Authority accepts that risk is ever present and is generally only willing to accept low levels of risk as part of its day to day business and in relation to its reputation. The Authority will normally only consider options where the level of risk can be managed to a low degree. However, the Authority may be willing to consider a higher level risk where it has the opportunity to be innovative in relation to its service delivery.

8 Risk Register

8.1 Risk registers should be maintained for all projects and significant pieces of work (Risk guidance in relation to projects is available form the Projects and Performance Team) . A corporate risk register and directorate risk registers are also maintained.

8.2 Significant risks identified should be included on the risk register in line with the table above. The template for the risk register is available from the Head of Governance and Support Services

TITLE OF RISK REGISTER & DATE

	IMPACT				
LIKELIHOOD	**Insignificant (1)**	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Catastrophic (5)**
Almost Certain (5)	5	10	15	20	25
Likely (4)	4	8	12	16	20
Possible (3)	3	6	9	12	15
Unlikely (2)	2	4	6	8	10
Almost Impossible (1)	1	2	3	4	5

9.   Roles & Responsibilities for delivering Risk Management

9.1   The table below sets out roles and responsibilities for different levels of people involved in delivering the Authority's Purposes and Duty:

Who	Roles & Responsibilities
Managers, employees and any person working with the Authority	• identify, assess and report risks within their areas • practice risk management in their day to day activities • identify the need for escalation of risks through their line manager
Managers	• oversee the effective implementation of risk management within their area in accordance with the agreed principles and framework • reflect significant changes to how they are operating and take actions to mitigate the likelihood and impact of risks • bring any escalated risks, which they are not able to manage at their level, to the Strategic Management Team's attention for rating in the Corporate Risk Register
Operational Management Team	• responsible for reviewing the Corporate Risk Register
Strategic Management Team	• responsible for the maintenance of a sound system of internal control • manage the strategic risks faced by the Authority • provide leadership and support to promote a culture in which risks are managed with confidence at the lowest appropriate level • accountable for ensuring that effective risk management and risk mitigation measures are in place to provide assurance to stakeholders • management of risks to the achievement of the Authority's objectives and provision of assurance that internal controls are effective within the Authority and across partnership working • Engage the public in the review and challenge of the Authority in the management of major activities, priorities and risks • promote the right culture in the workforce, including with volunteers and partners to encourage well thought through risk taking
Policy and Resources (P&R) Committee	• To ensure the robustness of risk management arrangements within the authority
Members	• Members have a role in ensuring decisions made include due regard to management of risks which affect the achievement of the Authority's objectives.

Glossary of Risk Management Terminology

- **Identification** (of risks) – Process to find and characterise risk

- **Mitigation of risk** – Process of selection and implementation of measures to mitigate or address risks. These could include:
  - Transfer the risk to a third party
  - Tolerate the risk. Do nothing as the investment in controls is judged to be likely to prevent the risk occurring or the risk is assessed as being so unlikely to materialise and further investment in controls offers poor value for money
  - Treat the risk. Agree controls to put in place to manage the risk
  - Take the Opportunity. Risk manage innovation or change for positive outcomes
  - Terminate the risk. Stop the activity or function in which the risk resides.

  - **Review and reporting (of risks)** – the process to determine the effectiveness of risk measures and the ongoing relevance of the risk

- **Risk** – the combination of the probability of an event and its consequences

- **Inherent Risk** – The risk that exists before any mitigations /control is put in place

- **Residual Risk** – The risk that remains after mitigations /Control is put in place

- **Risk Escalation** – Report a risk which exceed the set risk appetite to the management level above

- **Risk Management** – co-ordinated activities to identify, prioritise and manage risks that could affect the achievement (positively or negatively) of objectives. It is done by evaluating the probability of an event and its consequences, identifying the measures the organisation already has in place to manage identified issues (risks), prioritising the risk and then taking any further action to control these risks effectively. The adequacy of the control measures should be monitored and the control measures reviewed as necessary. Implementation of risk management strategies should result in more effective strategic planning, better utilisation of resources and better cost control.

- **Risk Management Principles** – set of high level principles to be uniformly observed in the implementation of risk management