# Risk management strategy

Louise Allen (October 2023)

## Introduction

1. Risk management is the process of identifying, assessing and controlling the uncertainties and opportunities associated with the delivery of the organisation's objectives. These uncertainties and opportunities can arise from events that are internal or external to the organisation.

2. To be effective, risk management should operate throughout the organisation. Strategic risk management focuses on the delivery of longer-term corporate objectives, for example, those set out in the Corporate Plan. Operational risks relate to the activities set out in the Operational Plan, and to specific project and activity plans.

3. At the broadest level, risk management is a system of people, processes and technology that enables an organisation to secure objectives in line with values and risks. Through our risk management processes we seek to apply resources to minimize, monitor and control the impact of negative events, while maximizing the opportunities offered by positive events. A consistent, and integrated approach to risk management operated throughout the organisation, at both strategic and operational levels, determines how best to identify, manage, and mitigate significant risks.

4. Those responsible for overseeing the delivery of the Park Authority's objectives need to establish their risk appetite, that is, the extent to which they are willing to accept a degree of uncertainty around strategic, and operational objectives. Our risk management approach seeks to evaluate risk, to determine the potential to reduce or mitigate these risks, and then to decide whether the remaining levels of risk are acceptable within the organisation's risk appetite.

## Risk management – underlying principles

5. The UK Government publication, *The Orange Book (Management of Risk – Principles and Concepts)* sets out the underlying principles to be applied by public bodies to the management of risk.

- Risk management shall be an essential part of governance and leadership, and fundamental to how the organisation is directed, managed, and controlled at all levels.
- Risk management shall be an integral part of all organisational activities to support decision-making in achieving objectives.
- Risk management shall be collaborative and informed by the best available information and expertise.
- Risk management processes shall be structured to include:
  a) risk identification and assessment, to determine and prioritise how the risks should be managed;
  b) the selection, design, and implementation of risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level;
  c) the design and operation of integrated, insightful, and informative risk monitoring; and
  d) timely, accurate and useful risk reporting to enhance the quality of decision-making, and to support management and oversight bodies in meeting their responsibilities.
- Risk management shall be continually improved through learning and experience.

## The management of strategic risks

6. Risk Management in the Park Authority is led from the strategic level. The Board agrees the long-term Corporate Plan for the organisation and establishes a strategic risk register identifying the main risks that could impact the achievement of the long-term priorities and objectives adopted within that Plan. The Board, with the support of officers, also establishes a set of mitigation actions focused on reducing the levels of uncertainty – whether the likelihood of a risk occurring, or its impact should it occur – to acceptable levels wherever possible.

7. The Board is responsible for managing the approach to strategic risk in delivery of its long-term goals and achieves this by integrating its review of the strategic risk position as an embedded element of its regular review of Corporate Plan delivery. The status of strategic risks is assessed twice each year at the same time as updates on delivery against strategic plans are presented by staff. Embedding these processes ensures the process of risk management remains relevant and directly linked to the process of monitoring delivery of the Authority's objectives.

8. The completeness of the Authority's risk register can be assessed at these points, as can the effectiveness of mitigation actions. Newly emerging uncertainties or opportunities and the planned approach to them can be added, while any risks that have been adequately reduced and are able to be evidenced as effectively managed and mitigated can be removed from the risk register.

9. Between Board meetings, the responsibility for monitoring strategic risk management and the coverage of the risk register and management action is delegated to the Board's Audit and Risk Committee. Both the Executive, and the Senior Management Team also undertake regular reviews of the risk register as an integral part of the wider risk management and assurance systems within the Park Authority.

## Risk appetite

10. Risk appetite is the level of risk that an organisation is prepared to accept in pursuit of its objectives before action is deemed necessary to reduce the risk. It represents a balance between the potential benefits of innovation and the threats that change inevitably brings. The ISO 31000 risk management standard refers to risk appetite as the "amount and type of risk that an organisation is prepared to pursue, retain or take". This concept helps guide an organisation's approach to risk and its management.

11. The Board communicates its appetite in relation to strategic risks, defining its position relative to each theme within the corporate plan. Appetite towards operational risks is determined by the Head of Service responsible for each theme within the operational plan.

12. Risk appetite will change over time, and according to circumstances. For example, financial constraints may result in less flexibility in the application of funds to meet objectives, and this may make us risk averse; funding at a level that allows us to be confident of financing all our objectives would make it easier for us to accept a higher level of risk. Consequently, risk appetite should be challenged periodically. As part of the quarterly review of the registers, consideration will be given to the appropriateness of the risk appetite parameters applied, given current circumstances, both within the Park Authority and externally in the wider environment.

13. Risk appetite determines the level of residual risk the organisation is willing to accept. For the purposes of risk evaluation, we consider risk appetite within 5 categories. Each of these categories is aligned with a risk score that defines the level of residual risk as set out in the table below:

| Category | Definition | Maximum residual risk score |
|---|---|---|
| Averse | Accept no risk / terminate risk. Actively limit and avoid risk. Avoid actions with any risk exposure. | 0 |
| Minimal | Minimise risk. Accept low level of risk in pursuit of strategic goals and priorities. Avoid innovation unless essential. | 3 |
| Cautious | Considered risk taking allowed, where benefits outweigh risks. Innovation generally avoided unless necessary. Preference towards safe delivery models with minimal uncertainty about benefits/loss. | 6 |
| Open | Take risk if expected reward warrants, within limits. Open to investment and innovation, with some loss accepted within limits. | 12 |
| Eager | Actively embrace innovation and change. Willing to accept risk/losses in the pursuit of exceptional benefits. | 25 |

14. Mitigation activities should be designed so as to reduce the original risk score to the desired value of residual risk.

## The management of operational risks

15. Management of operational risks is the responsibility of the Senior Management Team. Each service, led by its Director and Head of Service, establishes an operational risk register, identifying the main risks that could impact on the achievement of the operational priorities and objectives adopted within the annual Operational Plan for which that service is responsible. Each service establishes a set of mitigation actions focused on reducing the levels of uncertainty which may impact on delivery plans, in respect of both occurrence and impact, to acceptable levels wherever possible.

16. The status of operational risks is assessed quarterly as a standing agenda item for the Operational Management Group. This quarterly review provides the opportunity to consider the completeness of the operational risk register, the potential interaction of risks and dependencies for mitigation actions between services, and the effectiveness of mitigation actions. Where there is concern that the likelihood and/

or, impact of a risk is increasing, or that mitigation actions are proving ineffective, the matter should be escalated to the Senior Management.

## Risk management process

17. The process of risk management involves risk identification, risk analysis and assessment, and risk mitigation and monitoring.

18. Risk identification is the process of identifying and assessing both threats to the organisation, its operations, and its workforce, and potential impacts from taking up identified opportunities. For example, risk identification may include assessing pressures on staff (additional workload may arise from the opportunity to undertake new projects), the impact of cyber security breaches, threats to species or conservation activities, and other potentially harmful events that could disrupt operations.

19. Risk analysis involves establishing the probability that a risk event might occur and the potential outcome or impact of each event. Risk evaluation compares the magnitude of each risk and ranks them according to prominence (likelihood) and consequence (impact).

20. Risk mitigation refers to the process of planning and developing methods and options to reduce threats to the Park Authority's objectives.

21. Risk management is a continuous process that adapts and changes over time. Repeating and continually monitoring the processes can help assure maximum coverage of known and unknown risks. The process starts at the planning stage of all programmes and projects. All plans and project developments are expected to be designed on a risk-managed basis. This requires both an awareness of strategic risk management actions and a more specific focus on the management of lower-level operational risks.

## Risk response strategies and treatment

22. There are five commonly accepted strategies for addressing risk. The process begins with an initial consideration of risk avoidance then proceeds to three additional methods of addressing risk (transfer, spreading and reduction). Ideally, these three methods are employed in concert with one another as part of a comprehensive strategy. Some residual risk may remain.

a) Risk avoidance - Avoidance is a method for mitigating risk by not participating in activities that may negatively affect the organisation. For example, not starting a particular activity or project would avoid the risk of loss.
b) Risk reduction - This method of risk management attempts to minimize the loss, rather than completely eliminate it. While accepting the risk, it stays focused on keeping the loss contained. An example of this is the purchase of an employee assistance programme as preventative care, and part of our commitment to the wellbeing of staff and reduction of risks caused by staff absence.
c) Risk sharing - When risks are shared, the possibility of loss/ disbenefit is transferred from the individual to the group. Much of the work of the Park Authority depends on collaboration with partners. Such partnership working is likely to involve the sharing of risk. For example, the Palladium partnership manages the risk associated with the private financing of peatland restoration, while the Park Authority manages reputational risk and innovation risk around community benefit models, procurement and community attitudes to land management.
d) Transferring risk - Contractually transferring a risk to a third-party, such as, insurance to cover possible property damage or injury, shifts the risks associated with the property from the owner to the insurance company. Motor vehicle insurance is included in our fleet agreements; we also ensure that members of staff using their own cars on Park Authority business are covered by their own personal insurance policy for business use.
e) Risk acceptance and retention - After all risk sharing, risk transfer and risk reduction measures have been implemented, some risk will remain since it is virtually impossible to eliminate all risk (except through risk avoidance). This is called residual risk.

## Risk management procedure

23. The Corporate Plan defines the organisation's objectives for the next planning period (e.g. corporate plan 2023-27). The Operational Plan sets out the objectives for the coming financial year. The uncertainties (risks and opportunities) associated with each objective within the plan are considered. It may be helpful to consider each objective against the specific categories of risk listed in Appendix 1. Strategic risks are likely to be distilled from the Corporate Plan, with the Operational Plan being the likely source of operational risks. However, the interaction between strategic and operational risks should be considered throughout the risk management process.

24. The process of risk identification and management should run in parallel with budget setting and budget management/ monitoring activities. Budget allocations should be

made with due consideration of costs that may arise from the need to manage/ mitigate the risks inherent in particular activities or projects.

25. The identified risks are analysed according to likelihood of occurrence and their potential impact; they are evaluated using the scoring matrix shown in Appendix 2. Possible scores range between 1, where likelihood is rare and impact negligible, and 25, where likelihood is very high, and impact is also very high. The allocated risk scores are then used to establish the relative importance of the population of risks, allowing focus to be given to the highest scoring risks, their management and mitigation.

26. Each risk is entered into the risk register. The controls currently in place to manage the risk are described, and the assessment of likelihood and impact are noted, along with the overall risk score. Actions to mitigate the risk are devised. Risk appetite is established, and target risk scores are evaluated according to this appetite, the overall target score indicating the measure at which the risk would be considered acceptable. Each risk is given an owner, who is responsible for its monitoring and management.

27. The risk registers record the risk trend, using a rating system as shown below:

| | |
|---|---|
| Managed | Managed risk: risk assessment that risk is effectively managed and no longer a strategic risk posing potential to inhibit achievement of corporate strategic objectives. Risk can be removed from risk register. |
| Decreasing | Decreasing risk: risk now assessed as having reduced likelihood and/ or impact as a consequence of risk mitigation action. |
| Static | Static risk: risk impact and likelihood is stable. Overall strategic risk assessment is stable indicating that strategic risk remains, requiring ongoing management and continued implementation of proposed mitigation and controls. |
| Escalating | Increasing risk: risk impact and/ or likelihood is increasing resulting in increasing risk of achievement of strategic objectives being inhibited. Management action, and possibly resource investment, required to address risk environment and possibly introduce new mitigation action, in order to reduce risk impact and/ or likelihood. |

28. The Operational Risk Register is monitored by the Operational Management Group (OMG). Each quarter, a report on operational risks, highlighting any changes in their assessment, evaluation, or mitigation, is presented to meetings of the Senior Management Team (SMT). The completeness of the register is also considered by the OMG, with any new risks added to the register and reported to SMT.

29. The Strategic Risk Register is monitored quarterly by the Senior Management Team. Consideration is given to the interaction between strategic risks and operational risks, with any consequent amendments made to the register.

30. The Strategic Risk Register is presented to each meeting of the Audit and Risk Committee for consideration and discussion.

31. The Board reviews the strategic risk position as an embedded element of its regular review of Corporate Plan delivery. The status of strategic risks is assessed twice each year at the same time as updates on delivery against strategic plans are presented by staff.

32. A summary of the risk management process is set out in Appendix 3.

## Escalation of risks

33. Where there is concern about an increase in the organisation's operational risk profile this should be escalated immediately to the Executive team. Increased risk may arise from factors affecting the likelihood or the impact of particular risks, or through the failure of mitigation measures. An increase in risk score that moves a risk between categories (low – moderate – high – very high) **must** be escalated.

| | |
|---|---|
| 1 - 3 | Low |
| 4 - 6 | Moderate |
| 8 - 12 | High |
| >12 | Very high |

## Embedding Risk Management

34. All plans and project developments are expected to be designed on a risk-managed basis. This requires both an awareness of strategic risk management actions and a more specific focus on lower-level operational risks and their management.

35. Papers taking proposals to the Board should highlight how the proposals interact with the strategic risk register. Their effect may be to contribute to the management of existing risks, to add new risks by presenting new untried opportunities, and/ or to add new uncertainties to the Authority's operations.

36. Delivery plans flowing from Board decisions, and from the Authority's operational plans, are expected to develop and follow core risk management approaches agreed by the Authority. Plans should establish the operational and delivery risks that may impact on the achievement of objectives. They should also include an evaluation of whether, and how, the planned activities help address strategic risk management.

## Appendix 1 – Risk categories

**Strategy risks** – Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (e.g. political, economic, social, technological, environment and legislative change).
**Governance risks** – Risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.
**Operations risks** – Risks arising from inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money.
**Legal risks** – Risks arising from a defective transaction, a claim being made (including a defence to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property).
**Property risks** – Risks arising from property deficiencies or poorly designed or ineffective/inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public.
**Financial risks** – Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.
**Commercial risks** – Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and/or failure to meet business requirements/objectives.
**People risks** – Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.
**Technology risks** – Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.
**Information risks** – Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.
**Security risks** – Risks arising from a failure to prevent unauthorised and/or inappropriate access to the estate and information, including cyber security and non-compliance with General Data Protection Regulation requirements.

**Project/Programme risks –** Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.
**Reputational risks –** Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations.
Failure to manage risks in any of these categories may lead to financial, reputational, legal, regulatory, safety, security, environmental, employee, customer and operational consequences.

# Appendix 2 – Risk scoring matrix

| Impact | Risk Profile | | | | |
|---|---|---|---|---|---|
| Very High | 5 | 10 | 15 | 20 | 25 |
| High | 4 | 8 | 12 | 16 | 20 |
| Medium | 3 | 6 | 9 | 12 | 15 |
| Low | 2 | 4 | 6 | 8 | 10 |
| Negligible | 1 | 2 | 3 | 4 | 5 |
| Likelihood | Rare | Low | Medium | High | Very High |

# Appendix 3 – Summary of the risk management process

| | |
|---|---|
| 1 | The uncertainties (risks and opportunities) associated with each objective within the corporate/ operational plan are considered. |
| 2 | Budget allocations are made with due consideration of costs that may arise from the need to manage/ mitigate the risks. |
| 3 | The identified risks are analysed according to likelihood of occurrence and their potential impact; they are evaluated using the scoring matrix. |
| 4 | Each risk is entered into the appropriate risk register (strategic/ operational). The controls currently in place to manage the risk are described, and the assessment of likelihood and impact are noted, along with the overall risk score. Actions to mitigate the risk are devised. |
| 5 | Risk appetite is established, and target risk scores are evaluated according to this appetite. |
| 6 | Each risk is given an owner, who is responsible for its monitoring and management. |
| 7 | The Operational Risk Register is monitored quarterly as a standard item on the agenda of the Operational Management Group (OMG). The completeness of the register is also considered by the OMG. |
| 8 | Each quarter, a report on operational risks is presented to meetings of the Senior Management Team (SMT). The report highlights any changes in the assessment, evaluation, or mitigation of existing risks, and also provides details of new risks added to the register. |
| 9 | The Strategic Risk Register is monitored quarterly by the Executive. Consideration is given to the interaction between strategic risks and operational risks, with any consequent amendments made to the register. |
| 10 | The Strategic Risk Register is presented to each meeting of the Audit and Risk Committee for consideration and discussion. |
| 11 | The Board reviews the strategic risk position as an embedded element of its regular review of Corporate Plan delivery. The status of strategic risks is assessed twice each year at the same time as updates on delivery against strategic plans are presented by staff. |