Audit and Risk Committee

08 February 2022
Agenda item number 12

Risk Management and Policy Report

Report by Senior Governance Officer

Summary

The Authority's Risk Management Policy has been reviewed and updated.

Recommendation

To approve the Risk Management Policy and recommend its adoption by the Broads Authority.

1. Introduction

1.1. The Broads Authority has a Risk Management Policy setting out our rules and standards for corporate and operational risk management which is scheduled to be reviewed and updated every two years. The policy guides staff in monitoring and managing risk on a day to day basis when planning or implementing activities.

1.2. The policy was last reviewed and adopted by the Authority in January 2020.

1.3. Management Team recently reviewed the policy and made some minor changes: these reflect the committee's decision to review the Corporate Risk Register on a more frequent basis.

1.4. A copy of the updated policy (with tracked changes) is attached at Appendix 1.

Author: Sara Utting

Date of report: 25 January 2022

Appendix 1 – Risk Management Policy

Risk management policy

1. Introduction

1.1. This document sets out the Broads Authority's rules and standards for managing strategic and operational risk, and guides staff in assessing, monitoring and managing risk on a day-to-day basis.

2. Defining risk

2.1. In this context, 'risk' refers to an uncertain event, or set of events, which may affect the Authority's ability to operate its business or achieve its aims and objectives. An 'uncertain event' is one that might happen, rather than one that will definitely happen or is happening already.

2.2. Each risk has the key dimensions of 'likelihood' and 'severity'. Likelihood is the probability the event will happen, while severity is the impact the event would have if it happened.

3. Managing risk

3.1. The Authority must be able to consider the risks that may threaten or affect the running of its business and delivery of its aims and objectives, and make sure it has controls and mitigation measures in place to minimise those risks.

3.2. The international standard for risk management (ISO 31000) sets out useful guidance on risk management, emphasising that it should be integral to all processes and for all staff. Good principles for managing risk are that:

- It needs to be systematic, structured and timely.
- It is based on the best available information, including historical data, stakeholder and customer feedback, forecasting and expert judgment. It should be tailored to the organisation's internal and external context and risk profile.
- It takes human and cultural factors into account, recognising that people's capabilities, behaviours and intentions can either help or hinder the organisation's objectives.
- It is transparent and inclusive, needing the timely and appropriate involvement of stakeholders and decision makers at each stage, and ensuring proper representation of all those affected.
- It needs to be iterative, dynamic and responsive to change, taking account of changes in the internal and external environment.
- It needs to demonstrate continuous improvement.

3.3. Not having risk management procedures in place could result in a failure to identify and monitor risks, or apply appropriate and proportionate mitigation measures. It is also important to bear in mind:

- Our stakeholder and public expectations that we manage risk effectively;
- the demands of legislation and external bodies, such as regulators and auditors;
- the value of risk management in making informed decisions about the effective use of capital and resources, and in reducing costly mistakes or firefighting;
- the desire to make the organisation a better and safer place to work, and for others to work with.

4. Roles and responsibilities

Audit and Risk Committee

4.1. The Audit and Risk Committee oversees the development and operation of risk management at a strategic level, and regularly reviews the Corporate Risk Register. The Committee does not review the Directorate Risk Registers.

Management Team

4.2. Management Team (MT) is responsible for monitoring and managing risk across the organisation and making sure we have effective policies and procedures in place. MT oversees the review of the Risk Management Policy and Corporate Risk Register, with support from the ~~Head of~~Senior ~~-~~Governance Officer. Any significant corporate issues relating to risk management are brought to the Audit and Risk Committee's attention.

Directors

4.3. Directors are responsible for making sure risk management is embedded into the work of their Directorates, that risk owners and all other staff are aware of its importance, and that appropriate mitigation measures are in place. Directors are also responsible for their Directorate Risk Registers, which focus on day-to-day operational activities. They will bring MT's attention to any concerns or instances where ineffective risk management is impacting on the Authority's business or the achievement of its key aims and objectives.

Risk owners

4.4. Risk owners are responsible for monitoring and managing their assigned risks on a day-to-day basis. They will review their risks ~~on a regular basis (~~ at least every six months~~ , or earlier where~~~~when circumstances change significantly)~~ and make sure the registers are updated accordingly. Risk owners will bring their Director's attention to any concerns or instances where ineffective risk management may be impacting on the Authority's business or the achievement of its key aims and objectives.

Other staff

4.5. Risk management is not a specialist activity or only for nominated 'risk owners'. It is a core part of everyone's job, and should be embedded throughout the organisation and its activities. A risk management assessment should be part of planning and implementing all activities, with risks identified and mitigation measures put in place.

5. Risk Registers

Types of register

5.1. The Authority maintains a strategic Corporate Risk Register. This is supported by operational Risk Registers for its Strategic Services Directorate, Operations Directorate and Chief Executive's Group.

5.2. The **Corporate Risk Register** sets out the 'across the board' risks that could threaten the Authority's core business and the way it operates. The Corporate Risk Register is maintained on the Authority's intranet.

5.3. **Directorate Risk Registers** identify risks that could threaten day-to-day operational activities. The Registers are maintained by each Director. Where a new risk identified within a Directorate has a revised risk score above 16 (high risk), it will automatically be referred to the Corporate Risk Register for monitoring by the Audit and Risk Committee and MT. If new mitigation measures put in place then reduce the risk's score to below 16 (moderate to low risk), the risk will be removed from the Corporate Risk Register, but retained on the Directorate register.

5.4. MT has overall responsibility for the registers, and risk owners are responsible for reviewing and updating their individual risks. Every risk should be reviewed before every Audit and Risk Committee meeting, ~~at least six monthly~~, or earlier where~~when~~ there is a significant change in circumstances, with a note in the register of the date the risk was last reviewed.

Format

5.5. All registers have the following information:

- Area impacted by the risk (people, finance, performance, reputation or assets)
- Risk name and description
- Date entered on risk register
- Initial risk scores (likelihood and severity)
- Tasks to mitigate the risk (controls/safeguards/precautions)
- Revised risk scores (likelihood and severity)
- Additional actions required
- Risk owner (by job title)

6. Assessing risk tolerance levels

6.1. The Authority assesses risk against the matrix and scoring descriptions in Tables 1 to 4. For each risk, the dimension scores of **likelihood** and **severity** are multiplied to produce an **initial risk score**. When mitigation measures are identified, the two dimensions are scored and multiplied again to produce a **revised risk score**. This score is categorised as being a low, medium or high **level of tolerance**.

Table 1

Risk scores matrix

Likelihood						
	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
		Severity				

Table 2

Likelihood definitions

Rating	Definition	Value
Highly likely	The event is expected to occur	5
Probable	The event will probably occur	4
Possible	The event may occur at some time	3
Unlikely	The event is not expected to occur in normal circumstances	2
Rare	The event may occur only in exceptional circumstances	1

Table 3

Severity definitions

Schedule	Cost	Performance and quality	Value
<2 weeks delay	<1% of budget	Cosmetic impact only	1 Insignificant
2 weeks to 1 month's delay	1%-<2%	Some minor elements of objectives affected	2 Minor
1 month to <2 months delay	2%-<8%	Significant areas of some objectives affected	3 Moderate
2 months to <4 months delay	8%-<12%	Wide area impact on some objectives	4 Major

Schedule	Cost	Performance and quality	Value
>4 months delay	>12% of budget	Significant failure resulting in the project not meeting its objectives	5 Extreme

Table 4

Risk level tolerance

Total score	Risk treatment
High 16-25 Red risk	Risks are so significant that risk treatment is mandatory
Medium 6-15 Amber risk	Risks require a cost benefit analysis to determine the most appropriate treatment
Low 1-5 Green risk	Risks can be regarded as negligible, or so small that no risk treatment is required

6.2. When a potential new action or objective is assessed for risk, MT will review the revised risk score suggested by the risk owner to make sure it is robust and reasonable.

6.3. Where a risk score is above the tolerance level of 16 (high risk), the Chief Executive will immediately bring the risk to the attention of the Chairman of the Authority and the Chairman of the Audit and Risk Committee.

7. Risk management tools

Risk identification

7.1. Identifying a new risk can happen at any time, but is most likely:

- when the Authority takes on a new responsibility, scheme or project;
- as a result of an unforeseen incident or event; or
- as part of the annual review of risks by MT or Directorate teams.

7.2. A number of tools can help with risk identification, including those outlined below.

PESTLE looks at factors outside the organisation that can influence it, and stands for:

- Political – government policy and stability
- Economic – employment rates, material costs and interest/exchange rates
- Social – demographics, cultural trends and changes in lifestyle
- Technology – innovation and development
- Legal – employment, health and safety legislation and regulations
- Environmental – climate, carbon footprint, sustainability, recycling, waste disposal

APRICOT looks at factors within the organisation that may be affected, and stands for:

- Assets – land, buildings, contents, materials and equipment
- People – safe working systems, health and welfare
- Reputation – poor media coverage, political embarrassment
- Information – IT failures
- Continuity of Operations – failure to deliver or poor service
- Targets – failure to meet strategic objectives and achieve value for money

Risk mitigation

7.3. Once a risk is identified, mitigation measures need to be considered. Initially, this can be defined simply as 'tolerate, transfer, treat or terminate'.

7.4. A new risk should be reported to the appropriate Director as soon as possible by any officer so it can be entered in the relevant Directorate Risk Register. The Director will then assess whether the risk should be entered in the Corporate Risk Register.

7.5. When a new corporate risk is identified, MT will assess the mitigating measures in place or proposed, and whether these will manage the risk to 'as low as reasonably practicable'. This process looks at whether the likelihood and severity of the risk is addressed adequately, and whether the Authority needs to enter into the risk, assuming it is optional, bearing in mind how the activity itself will further the Authority's objectives and the level of risk associated with it.

8. Review timetable

8.1. In addition to the regular review by risk owners, MT will review the Corporate Risk Register ~~every six months~~regularly to consider whether:

- the identified risks are appropriate and up-to-date
- the actions and controls in place are adequate and appropriate
- the revised risk score is appropriate
- any additional action is needed to help mitigate the risk
- any new risks should be added to the Register, either for new activities or for existing activities where the risk level may have increased.

8.2. The Corporate Risk Register will be reviewed regularly~~at every meeting of by~~ by the Audit and Risk Committee ~~twice a year~~. Where a risk score has increased, the reasons for the change will be set out.

Policy updated: January 2022~~0~~
Next update due: January 2024~~2~~

Contact officer: ~~Head of Governance~~~~Director of Finance~~ Senior Governance Officer