Audit and Risk Committee

19 November 2019
Agenda item number 11

Risk management register and policy: Update

Report by Head of Governance

Summary

The Authority's Corporate Risk Register (previously called the Strategic Risk Register) and Risk Management Policy have been reviewed and updated.

Recommendation

To approve the updated Corporate Risk Register and Risk Management Policy.

1. Background

1.1. The Broads Authority's Corporate Risk Register was reviewed and updated in October 2019 (Appendix 1). The Register focuses on high level strategic risk, with more detailed operational level risks contained in separate Directorate Risk Registers.

1.2. In this Corporate Risk Register ten risks are identified under the core areas of people, finance, assets, performance and reputation. Each risk is scored for likelihood and severity, and the two scores multiplied to produce an initial risk score. Each risk is then scored again, with mitigation measures in place, to produce a revised risk score.

1.3. The revised risk scores show that eight risks are assessed as 'medium risk' and two as 'low risk'. No high risks are identified. In all cases, applying mitigation measures has reduced the initial risk scores.

1.1. The Authority also has a Risk Management Policy setting out our rules and standards for corporate and operational risk management, and this has been updated. The policy guides staff in monitoring and managing risk on a day-to-day basis when planning or implementing activities. The updated policy is at Appendix 2.

Author: Maria Conti

Date of report: 22 October 2019

Appendix 1 – Corporate Risk Register

Appendix 2 – Risk Management Policy

Appendix 1 - Corporate Risk Register (Aug 2019)

Impact area People, finance, assets, performance, reputation	**Risk no.**	**Risk name** Risk that may affect the BA	**Risk description** Impact on delivery of BA objectives, service delivery, reputation	**Date entered on risk register**	**Initial likelihood** Score 1-5	**Initial severity** Score 1-5	**Initial risk score** Likelihood x severity	**Tasks to mitigate risk** (controls/safeguards/precautions) What we have done to date, noting any other factors that may influence the risk	**Revised likelihood** Score 1-5	**Revised severity** Score 1-5	**Revised risk score** Likelihood x severity	**Additional actions required** What we plan to do within the next year	**Risk owner** Officer ultimately responsible for the risk
People	1	Loss of knowledge and expertise	Loss of knowledge, expertise or working associations, due to key staff leaving or not being available for long periods	19/8/2019	4	4	High risk 16	Plan in place for handover period when key staff leave BA or are absent for significant periods HR polices in place to support staff retention Reviewing electronic data storage to support access to any officer's files Business Continuity Plan in place with system back up	3	3	Medium risk 9	Continue Data Project to ensure access to all staff e-folders Draft resilience plan for key staff and services (by summer 2020) Review Business Continuity Plan (by end 2019)	Chief Executive
Reputation	2	Harmful actions undermining public confidence in Broads Authority	Damage caused by comments or actions by BA Member or Officer, with consequent harm to relationships with key stakeholders or undermining of public confidence in BA	19/8/2019	2	4	Medium risk 8	Code of Conduct for Members in place containing Nolan Principles of Conduct Code of Conduct for Officers in HR policies Training on Code of Conduct provided to all Members Protocol on Member and Officer Relations in place (updated May 2017) Proactive communication policy with local media and social media	2	3	Medium risk 6	Review and rewrite constitutional and corporate documents to make them shorter and clearer	Chief Executive
Assets	3	Loss of key physical assets	Damage, loss or malfunction to key assets impacting on BA functions/duties (e.g. navigation, moorings, Mutford Lock, rail bridges, Port of Norwich) that would impact public access/services	19/8/2019	3	4	Medium risk 12	Asset Management Strategy in place Integrated Access Strategy and Moorings Strategy in place (updated 2019) BA attendance at Network Rail meetings Insurance in place for equipment and buildings over £250. Cover includes business interruption. Landowner negotiations processes in place Programmed inspection regime in place and regular maintenance carried out	3	2	Medium risk 6	Implement action plan to consolidate network of mooring provision across system Engage in meetings with Norfolk County Council, New Anglia and Network Rail about Trowse bridge and rail swing bridges	Director of Operations
Finance	4	Reduction in income	Uncertainty on how BA will be funded from 1 April 2020 by DEFRA, as well as toll income uncertainty. Any reduction would impact our ability to deliver our duties.	19/8/2019	3	5	Medium risk 15	Regular contact with Government (DEFRA) to follow up on Comprehensive Spending Review Regular input to Government consultations Landscapes Review – positive proposals about maintaining at least current funding levels Prudent budgeting for Navigation and National Park expenditure. Reserves in place to mitigate against sudden drop in income. Some significant blocks of work delivered through	2	3	Medium risk 6	Model expenditure options depending on proposed grant settlement and toll increases. Negotiate with DEFRA when timings are known, including joint response from English National Parks	Chief Financial Officer

Impact area People, finance, assets, performance, reputation	**Risk no.**	**Risk name** Risk that may affect the BA	**Risk description** Impact on delivery of BA objectives, service delivery, reputation	**Date entered on risk register**	**Initial likelihood** Score 1-5	**Initial severity** Score 1-5	**Initial risk score** Likelihood x severity	**Tasks to mitigate risk** (controls/safeguards/precautions) What we have done to date, noting any other factors that may influence the risk	**Revised likelihood** Score 1-5	**Revised severity** Score 1-5	**Revised risk score** Likelihood x severity	**Additional actions required** What we plan to do within the next year	**Risk owner** Officer ultimately responsible for the risk
								external funds won by BA					
Performance	5	Not meeting statutory duties or requirement of external legislation	Underperformance of, or conflict between statutory purposes resulting in legal issues and/or negative impacts (e.g. contravening Habitats Directive, loss of navigation)	19/8/2019	3	5	Medium risk 15	Professional staff trained and diligent in protecting ecology and the environment Detailed processes in place including Environmental Standard Operating Procedures Collaborative working in place with key stakeholders to understand and address issues and risks Officer level project boards in place with Wildlife Trusts, Natural England and Environment Agency to monitor progress and ensure compliance to statutory regulations Scientific research and monitoring ongoing to assess impacts and mitigation measures developed if potential harm identified.	2	2	Low risk 4	Review aquatic plant cutting regime and standards required	Chief Executive
Performance	6	Not meeting statutory duties as a local planning authority	Underperformance of planning function resulting in legal issues and/or negative impacts on our reputation	19/8/2019	3	4	Medium risk 12	Statutory duties identified as part of appraisal process with key staff Staff training Planning delivery monitored formally (Planning Committee review performance quarterly and appeals annually)	2	4	Medium risk 8	Continue to monitor delivery	Director of Strategic Services
People	7	Safety incidents	Death or serious injury to staff, volunteer or member of public while carrying out operational works	19/8/2019	5	5	High risk 25	Health and safety policies in place and reviewed regularly by H&S Committee and risk owners Safety Committee monitors and reviews incident reports and risk assessments reviewed and updated regularly All staff and volunteers trained in key H&S issues, regular tool box talks given before carrying out tasks Safety Observations - ONS system in place to catch near misses and learn from incidents. All accidents investigated. Regular audits used to check control measures. Insurance in place for legal expenses Quarterly reports on Health and Safety Monitoring assessed by Management Team	2	5	Medium risk 10	Monitor changes in H&S legislation Monitor industry best practice and implement changes where required	Director of Operations
Reputation	8	Disruption in key partnerships	Failure to deliver projects on time and within budget leading to potential financial issues, lack of service delivery or adverse publicity	19/8/2019	3	4	Medium risk 12	Contractual arrangements in place for key partnerships (see Partnership Register) Regular project progress reports taken to BA members Proactive role maintained within formal and	3	3	Medium risk 9	Review and update Partnership Register – by Nov 2019 Develop risk register for UK NP comms team	Chief Executive

Impact area People, finance, assets, performance, reputation	**Risk no.**	**Risk name** Risk that may affect the BA	**Risk description** Impact on delivery of BA objectives, service delivery, reputation	**Date entered on risk register**	**Initial likelihood** Score 1-5	**Initial severity** Score 1-5	**Initial risk score** Likelihood x severity	**Tasks to mitigate risk** (controls/safeguards/precautions) What we have done to date, noting any other factors that may influence the risk	**Revised likelihood** Score 1-5	**Revised severity** Score 1-5	**Revised risk score** Likelihood x severity	**Additional actions required** What we plan to do within the next year	**Risk owner** Officer ultimately responsible for the risk
								informal partnerships					
Data security	9	Breach in data protection or loss of data	Failure by staff to follow IT and/or GDPR processes or protocols resulting in in-built security being bypassed and allowing data loss, data breach or cybercrime to BA systems	19/8/2019	4	4	High risk 16	Training in cybercrime given to all budget holders Certified GDPR Data Protection Officer(s) in place Data Protection training given to staff	2	4	Medium risk 8	Review GDPR Compliance Plan Monitor and review case law and keep up to date with GDPR and data protection information/ best practice	Director of Operations
Finance	10	Projects externally funded by EU post-Brexit	Failure to get reimbursement for expenses occurred for projects funded by EU in event of no-deal Brexit scenario	19/8/2019	2	4	Medium risk 8	Detailed Risk Register for CANAPE reviewed at least twice a year by Steering Group with entries related to Brexit Regular contact made with Joint Secretariat of North Sea Programme Regular reports on CANAPE taken to BA members Treasury has guaranteed funding for all organisations where EU funded project was approved before Brexit	2	2	Low risk 4	None	Director of Strategic Services

Prepared by: Management Team and Head of Governance
Date updated: 19 August 2019
Next update due: 19 February 2020

Appendix 2 - Risk Management Policy

1. Introduction

1.1 This document sets out the Broads Authority's rules and standards for strategic and operational risk management. It also guides staff in the monitoring and management of 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 two key dimensions - 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. It emphasises that risk management creates and protects value by contributing to the organisation's objectives and improving its performance, efficiency, governance and reputation. As such, it should be integral to all processes and for all staff.

3.3 Some good principles for managing risk are that:

- It needs to be systematic, structured and timely.
- It is based on the best available information – 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.
- Finally, it needs to demonstrate continuous improvement.

3.4 Not having risk management procedures in place could result in a failure to identify and monitor risks or have appropriate and proportionate mitigation measures. When assessing risk, it is also important to bear in mind:

- the expectations of stakeholders and the public that risk will be managed effectively;
- the demands of legislation and external bodies, such as regulators and auditors;
- the value of risk management in helping to make better informed decisions in the effective use of capital and resources;
- the reduction in costly mistakes, re-work and fire-fighting that can arise from effective risk management; and
- the desire to make the organisation a better and safer place to work and with which to do business.

4. Roles and responsibilities

Audit and Risk Committee

4.1 For the Authority, the Audit and Risk Committee oversees the development and operation of risk management at a strategic level, and reviews the Corporate Risk Register on a regular basis.

Management Team

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

Directors

4.3 Directors are responsible for making sure risk management is embedded into the work of their Directorates, and that risk owners and other staff are aware of its importance and have appropriate mitigation measures in place. Directors are also responsible for their Directorate Risk Registers, which focus on day-to-day operational activities and link up to the Corporate Risk Register. Directors 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 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 just 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 implementation for 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 and operational Directorate Risk Registers for Strategic Services, Operations and Chief Executive's Group.

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

5.3 **Directorate Risk Registers** identify risks that could threaten day-to-day operational activities. Where a risk identified within a Directorate has a revised risk score above 16 (high risk), it will automatically be referred to the Corporate Risk Register. The Registers are maintained by each Director.

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

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 priorities or 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 formally review the Corporate Risk Register every six months 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 also be reviewed by the Audit and Risk Committee twice a year. Where a risk score has increased, the reasons for this change will be set out.

Date of review: 17 October 2019
Date of next review: October 2021
Contact officer: Head of Governance