Audit and Risk Committee

21 July 2020
Agenda item number 13

Corporate Risk Register – 6-month review

Report by Head of Governance

Summary

The Broads Authority's Corporate Risk Register (formally known as the Strategic Risk Register) has been reviewed and updated. The Directorate Risk Registers and the Risk Management Policy have also been reviewed and updated.

Recommendation

To approve the updated Corporate Risk Register.

1. Risk Registers

1.1. The Audit and Risk Committee's responsibilities for risk are set out in the Committee's Terms of Reference. For the Corporate Risk Register (previously called the Strategic Risk Register), these are to make sure the Register adequately addresses the Authority's risks and priorities; to monitor the effective development and operation of the Authority's risk management; and to monitor progress in addressing risk-related issues reported to the Committee, and seek assurance that risks are being managed within the risk appetite of the Authority.

1.2. The Corporate Risk Register (Appendix 1) sets out the 'across the board' risks that could threaten the Authority's core business and the way it operates.

1.3. Below this are Directorate Risk Registers, which identify risks that could threaten day-to-day operational activities. These Registers are managed by each Director. Where a new risk identified within a Directorate has a revised risk score above 16 (high risk), it is automatically referred to the Corporate Risk Register for monitoring by the Audit and Risk Committee and the Management Team. 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.

1.4. The Management Team has overall responsibility for the registers, and risk owners are responsible for reviewing and updating their individual risks. Every risk is 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. The registers are maintained on the Authority's intranet.

2. Review of Corporate Risk Register – July 2020

2.1. The six-month review of the Corporate Risk Register is at Appendix 1. A new risk has been added to the register in light of the current pandemic situation.

3. Risk Management Policy

3.1. The Risk Management Policy (Appendix 2) was reviewed and updated in January 2020. The policy sets out the Authority's rules and standards for managing strategic and operational risk, and guides staff in assessing, monitoring and managing risk.

Author: Maria Conti

Date of report: 07 July 2020

Appendix 1 – Corporate Risk Register (July 2020)

Appendix 2 – Risk Management Policy

Broads Authority Corporate Risk Register (July 2020)

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 key staff knowledge and expertise	Loss of knowledge, expertise or working associations, due to key staff leaving the BA 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 policies and procedures in place to monitor absence and to support staff retention Electronic data storage being reviewed 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 2020)	Chief Executive
Reputation	2	Harmful actions undermining public confidence in BA	Damage caused by comments/actions by BA Members or Officers, with consequent harm to relationships with 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 and training given to all Members Code of Conduct for Officers in HR policies Protocol on Member and Officer Relations in place Proactive communication policy with local media and social media in place New Monitoring Officer and Deputy Monitoring Officer appointed, with specialisms in Local Authority governance.	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 and affecting public access or services (e.g. navigation, moorings, Mutford Lock, rail bridges, Port of Norwich)	19/8/2019	3	4	Medium risk 12	Asset Management Strategy in place Integrated Access Strategy and Moorings Strategy in place (updated 2019) Legal undertaking and regular meetings in place with Network Rail regarding rail bridge maintenance BA attendance at Network Rail meetings Insurance in place for equipment and buildings over £250. Cover includes business interruption. Landowner negotiations processes in place	3	2	Medium risk 6	Implement action plan to consolidate network of mooring provision across system	Director of Operations

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
								BA in Working Group with Norfolk County Council, New Anglia and Network Rail regarding Trowse bridge and rail swing bridges Programmed inspection regime in place and regular maintenance carried out					
Finance	4	Reduction in income	Uncertainty about BA funding from Defra from 1/4/21 and toll income, as any reduction would affect our ability to deliver our duties. Loss of money as a result of fraud incident against the BA, including cybercrime.	19/8/2019	3	5	Medium risk 15	Regular contact with Government (DEFRA) regarding Comprehensive Spending Review and COVID-19 impacts Regular input to Government consultations Prudent budgeting for Navigation and National Park expenditure. Reserves in place to mitigate against sudden drop in income. Savings identified with budget holders to ease some of COVID-19 pressures. Some significant blocks of work delivered through external funds won by BA Training in cybercrime given to all budget holders	2	3	Medium risk 6	Model expenditure options depending on proposed grant settlement and toll increases. Reviewing impact of COVID-19 on boat numbers and levels of reserves. Conclude agreement with DEFRA underwriting deficit in navigation income. Achieve cyber essentials accreditation	Chief Financial Officer
People	5	Impact on people's health	Significant public health crisis whereby imposed measures prevent visitors accessing the Broads for prolonged period	02/07/2020	5	5	High Risk 25	Strict adherence to Government guidance and mitigation measures Yare House, TICs and remote offices and facilities all risk assessed Maintain key services (Safety Management) within the Broads executive area Clear and concise internal and external communications Immediate meeting of key staff to determine appropriate actions, services and measure required to react to crisis Broads Authority convened to establish emergency powers and delegated powers needed to run the Authority	5	4	High Risk 20	Review of key services, budgets and reserves to safeguard Broads Plan delivery and externally funded projects	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
								Communication with relevant Government Departments to assess measures, clarify advice and safeguard funding					
Performance	6	Not meeting BA statutory purposes or the requirements of external legislation related to those statutory purposes	Underperformance in achieving, or conflict between, our statutory purposes, resulting in legal issues or adverse impacts on the Broads and stakeholders (e.g. contravening Habitats Directive, loss of navigation)	19/8/2019	3	5	Medium risk 15	Provision of external legal services and Monitoring Officer (MO) in place Constitutional documents in place Strategic plans and Broads Local Plan subject to Sustainability Appraisal and Habitats Regulations Assessment Detailed environmental practices in place, including Environmental Standard Operating Procedures Collaborative working ongoing 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 with statutory regulations Scientific research and monitoring ongoing to assess impacts, and mitigation measures developed if potential harm identified.	2	2	Low risk 4	Monitor external legal and MO services. Develop timetable for Broads Plan review	Chief Executive
Performance	7	Not meeting statutory duties as a local planning authority	Underperformance of planning function resulting in legal issues/ negative impacts	19/8/2019	3	4	Medium risk 12	Statutory duties identified as part of appraisal process with key staff Staff training in place 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	8	Safety incidents resulting in death or serious injury	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	2	5	Medium risk 10	Monitor changes in H&S legislation Monitor industry best practice and implement changes where required Review Codes of Practice to maintain	Director of Operations

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
								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 Safety System externally audited to ensure fit for purpose and compliance.				operational suitability and safety end 2020 Safety Officer to carry out internal review of key H&S legislation to ensure BA processes are appropriate (end 2020)	
Reputation	9	Disruption in key project 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 Partnerships Register) Regular project progress reporting to BA members Proactive role maintained within formal and informal partnerships at officer and member level Regular meeting with funders to discuss progress and highlight issues in timing or delivery	3	3	Medium risk 9	Review and update Partnerships Register (by Nov 2020) Develop risk register for UK NP Comms Team	Chief Executive
Performance	10	Breach in data security or 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 or data breach	19/8/2019	4	4	High risk 16	Data/IT systems secured through firewalls, anti-virus software, password and security policies, online training for staff and HR policy Bi-annual internal audit of IT systems and processes carried out Certified GDPR Data Protection Officer(s) and GDPR Compliance Plan in place, and data protection training given to all staff ICT reviewed IT security protocols as staff working from home to ensure compliance	2	4	Medium risk 8	Monitor and review case law and keep up to date with GDPR and data protection information/ best practice Provide refresher GDPR & Data Protection online training via ELMS to all staff (by end 2020)	Director of Operations

Prepared by: Management Team, Head of Governance
Date updated: July 2020
Next update due: January 2021

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.

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 Governance. 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 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 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

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 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 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 update: January 2020
Contact officer: Head of Governance