GEDLING BOROUGH COUNCIL

INTERNAL AUDIT REPORT - FINAL

RISK MATURITY
AUGUST 2021

IDEAS | PEOPLE | TRUST

BDO

Distribution	
Alison Ball	Director of Corporate Services and Section 151 Officer
Paul Adcock	Head of Finance and ICT

Report Status list	
Auditors:	James Savigar
Dates work performed:	24 May – 14 July 2021
Draft report issued:	21 July 2021
Final report issued:	23 August 2021

EXECUTIVE SUMMARY

OVERVIEW

The purpose of the risk maturity assessment is to help ensure an effective risk management culture becomes embedded across the Council, by highlighting areas where processes could be improved. As a primarily advisory piece of work, the assessment will not generate an assurance opinion. The Council's ambition is to achieve the risk enabled status.

Per the Council's Risk Management Strategy all managers and officers are encouraged to raise and escalate any risks or concerns. The Council maintains its risk registers on excel spreadsheets through a quarterly update and review process. The process is led by Heads of Service and supported by the Insurance and Risk Management Officer. Once the quarterly update is complete the registers are submitted to the Senior Leadership Team (SLT) for review and discussion.

We considered the maturity of the Council's current risk management arrangements by assessment against BDO's risk maturity model. The following elements were assessed:

Risk Governance	Risk Assessment	Risk Mitigation	Monitoring and Reporting	Continuous Improvement
- Strategy and objectives - Tone at the top - Roles and responsibilities - Resources - Training - Risk appetite - Risk strategy - Risk Policy	- Risk Identification - Risk Analysis - Risk Evaluation - Assigning responsibilities for risks	- Current Mitigation - Action Plans - Reaction Plans	- Monitoring - Reporting - Assurance	- Review Approach - KPIs

The current and target levels of maturity for each area were assessed in accordance with five categories, defined at Appendix III:

Naïve	Aware	Defined	Managed	Enabled

The Risk Maturity Assessment Matrix is at Appendix III and sets out the definitions for each level of maturity. It is the intention that the results of the assessment assist those charged with governance in the further development of an effective and embedded risk management framework. Within our report we have identified areas where further development is required in order to reach the target maturity levels and have made recommendations for improvement within the body of the report. We have summarised below the current and target maturity levels, based on our work performed and the planned trajectory of progress for the Council.

	Risk Governance	Risk Assessment	Risk Mitigation	Monitoring and Reporting	Continuous Improvement
Current	Defined	Defined	Aware	Aware	Defined
Target	Managed	Managed	Managed	Managed	Managed

GOOD PRACTICE:

In our review, we have noted the following areas of good practice:

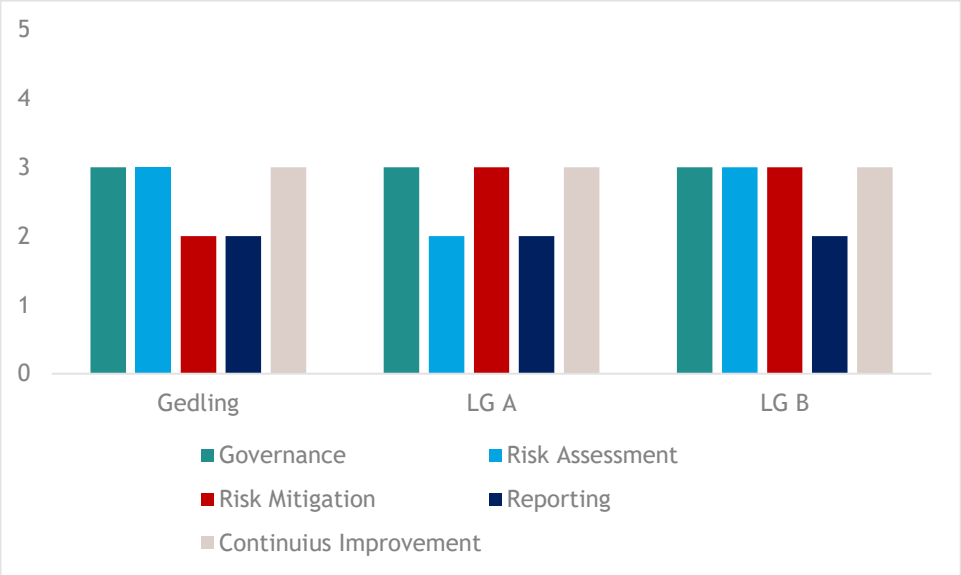
- The Council has clearly documented its strategic objectives within the Gedling Plan 2020 – 2023 and published this on its website. The Council also has a robust annual service planning process and established golden thread methodology to ensure service plans are in place to support the achievement of the Gedling Plan
- A Risk Management Strategy and Framework has been documented which clearly defines the Council's risk appetite
- The risk registers are formatted to ensure the key drivers of each risk are clearly documented
- All of the risks on the register have been assigned a risk owner who is responsible for overseeing the effective management of the risk
- There is an established quarterly review process for the corporate risk register with progress on each risk being recorded on a consistent basis each quarter and reported to the SLT. This is evidenced in the meeting minutes and reports of the SLT meetings.

KEY FINDINGS:

Recommendations have been raised against each of the areas of the risk maturity assessment. However, the key findings have been noted below.

- Our interviews with heads of service identified that there may not be a full understanding of risk management amongst officers below manager level, with a reluctance to discuss the topic of risk with them due to more junior staff perceiving risks as a negative. There is no risk management training programme within the Council to provide its officers and members with the knowledge and skills to effectively understand and manage risk throughout the organisation
- The roles and responsibilities of officers below manager level for managing risks are not clearly defined within the Risk Management Strategy and Framework
- Risk recorded on risk registers are not linked to objectives or categorised by risk type.
- Risks recorded on the risk register are not described to a consistently high standard to provide the reader with an understanding of the risk, its cause and the consequence should the risk materialise
- Controls and actions to mitigate risks are not documented to a suitably high standard to provide the reader with assurance that the risk is being effectively managed. Actions are not recorded as SMART (specific, measureable, attainable, realistic and timebound) actions, particularly in the service risk registers where actions are not assigned implementation dates
- Reviews of risk registers by the heads of service are not recorded on a consistent basis each quarter, with these sections of the risk registers often left blank.

Having conducted a number of Risk Maturity Assessments at other Councils, we have identified that the Council scores approximately in line with the average against the key indicators included within the report when compared to the other authorities we have reviewed (see graph below for further detail). There are areas for improvement across the Council's risk management function, particularly with regards to the quality of the documentation of risks, controls and actions within registers and the consistency of recording updates for each of these risks. Therefore, if ongoing efforts to improve the risk management function continue, and the targets identified throughout the report are met by implementing the recorded actions, the Council will be able to exceed the average across the other authorities.



ASSESSMENT OF RISK MATURITY AGAINST THE BDO RISK MATURITY MODEL

Risk Maturity Assessment – Governance			
1.	**Strategy and objectives:**	**✓/✗**	**Evaluation**
1.1	The organisation has clear objectives	✓	The Council has set out its key objectives in the Gedling Plan 2020 – 2023. This plan sets out the Organisation's vision, ambition, values and priorities. There are five priorities as follows: • Cohesive, Diverse and Safe Communities • High Performing Council • Vibrant Economy • Sustainable Environment • Healthy Lifestyles. The plan goes on to set out the specific steps the Council will take to achieve these priorities over the three years to 2023. This plan can be found on the Gedling Borough Council (GBC) website.
1.2	Division / department objectives are set and linked to the organisation's objectives.	✓	The Council takes a Golden Thread approach to ensure that its objectives and priorities are incorporated in to service plans throughout the organisation. This involves an annual business planning process with the heads of service working with the senior leadership team to develop a comprehensive plan for the year to enable the steps within the Gedling Plan to be achieved. This approach is also documented and available on the GBC website.
2.	**Tone at the top**		
2.1	The Council have mandated that a formal approach be taken to risk management and set out why risk management is important.	✓/✗	The Council has documented a Risk Management Strategy and Framework which includes a section titled Risk Methodology. This clearly sets out the Council's approach to risk management and how its officers are expected to apply the framework. When conducting interviews with the heads of service they had a clear understanding of the processes they were expected to follow and the Council's overall approach to risk management. However, they also identified that officers below manager level do not always have the same level of understanding. The interviews highlighted that there is a tendency to shield these junior staff from risk and the formal processes for managing risk. We were also told that when having discussions with officers below manager level the managers or heads of service will deliberately avoid using the word risk in order to avoid 'worrying' these officers with potential risks.
3.	**Roles and responsibilities:**		
3.1	Roles and responsibilities for risk management have been defined centrally and across divisions and departments.	✗	As per the above, the Council's Risk Management Strategy and Framework highlights all key roles and responsibilities for risk management. These are documented in the Risk Methodology section where the specific actions expected of the different grades of staff are communicated and also in Appendix 2 of the strategy which sets out the higher level responsibilities of each of these grades. However, as with the above these roles and responsibilities do not stretch as far as officers below manager level, with the documented roles and responsibilities stopping at the manager or team leader level.

3.2	Effectiveness in discharging risk management responsibilities is evaluated as part of individual performance review/appraisal.	✓/×	Whether an individual will have their effectiveness at discharging risk management responsibilities assessed during their appraisal will depend on whether they have specific objectives set relating to risk management. This will be the case for heads of service who have overall responsibility for the day to day performance of risk management functions within their service. However, this is less consistent across other officers despite the Risk Management Strategy and Framework clearly defining the risk management responsibilities of these individuals.
4.	**Resources:**		
4.1	Resource requirements have been identified and budget allocated.	✓	The administration of the risk management function is supported by the Insurance and Risk Management Officer who is able to support the heads of service in the quarterly process of reviewing and updating risk registers. The risk registers themselves are maintained in a simple format on excel spreadsheets. Our discussions with the Council's officers identified that this system works well and there is no appetite for a more complex dedicated risk management system. Time and resources of the Senior Leadership Team are also budgeted and allocated to risk management via quarterly review and discussion of the corporate and service risk registers.
4.2	Regular review takes place of ongoing resource requirements.	✓	Our interviews with the heads of service and Insurance and Risk Management Officer identified that there is regular discussion and consideration of the resources needed to address specific risks and implement mitigating actions. The Council's overall resources to manage risk are also evaluated on an ongoing basis when new information is highlighted that could impact risk management within the organisation.
5.	**Training:**		
5.1	Training undertaken for managers and staff responsible for risk management.	×	The Risk Management Strategy and Framework identifies that 'there will be a need to provide training and development on risk' and that 'the precise nature and timing of the training will be dependent upon the needs of individual staff groups and the availability of resources.' However, our discussions with the heads of service and Insurance and Risk Management Officer identified that there has been no recent training of a specific risk management nature delivered to staff or members. Whilst our interviews identified that the heads of service themselves are comfortable with and aware of their responsibilities within the risk framework, there is a concern that the staff within their teams lack a full understanding of risk management and further training and education on this topic would be beneficial.
5.2	Training in risk management is provided to all staff.	×	
6.	**Risk Appetite:**		
6.1	A formal risk appetite statement has been agreed by the Council at a corporate level	✓	The Risk Management Strategy and Framework includes a risk appetite statement. This sets out how the Council uses three bands to assess risk (red, amber, green) which determines the prioritisation and the approach it will take to manage each risk. Each band is defined in the Framework.

6.2	Risk appetite statements are in place and within departments.	✗	Services do not have their own risk appetite statements. The Risk Management Strategy and Framework acknowledges that different decision making groups will have different attitudes to risk and that by having one central risk appetite statement for the organisation improves the consistency and objectivity of risk management.
7.	**Risk Strategy:**		
7.1	A risk management strategy is in place which is signed off by the Council	✓/✗	A Risk Management Strategy and Framework was last updated in July 2017 and was due for review and update in July 2020 which is overdue. The Strategy is comprehensive in setting out the purpose and objectives of risk management, the Council's risk appetite and what the strategy aims to achieve to manage risks within the organisation.
8.	**Risk policy:**		
8.1	A risk management policy is in place and has been communicated throughout the organisation.	✓/✗	As above, there is a comprehensive Risk Management Strategy and Framework in place, although it is currently overdue for review. The Framework clearly sets out the approach taken by the Council to manage risk, including an explanation and detailed procedure for how risks should be identified, assessed and reported.

Assessment of maturity for this element					
	Naïve	Aware	Defined	Managed	Enabled
Current			✓		
Target				✓	

Risk Maturity Assessment – Risk Assessment			
1.	**Risk Identification:**	**✓/✗**	**Evaluation**
1.1	Comprehensive process in place for systematically identifying risks throughout the organisation.	✓/✗	The Risk Management Strategy and Framework provides guidance on the identification and categorisation risk. This is as follows: Risks will be considered under the major type headings of 'Strategic', 'Operational', 'Partnership' and 'Project' and within those under the broad categories: • Financial • People • Assets • Legal • Customer & Reputation • External Environment. This guidance is limited however and does not go in to the detail of the methods officers should use to assist them with the identification of risk. Our interviews found that heads of service make use of the annual service planning process to identify potential risks at an early stage. Also, if there is a specific project being planned then the risks associated with this project are identified at the project planning stage. Otherwise, the Council relies on its officers' knowledge of their service and the wider environment to identify the relevant risks with limited guidance or procedure to facilitate the systematic identification of risk.
2.	**Risk Analysis:**		
2.1	Risks are linked to objectives	✗	Risks recorded on the registers are not linked to objectives within the Gedling Plan or the individual service plans, although risks on individual service registers are linked to the risks on the corporate register.
2.2	Risks are clearly described	✗	The quality of risk descriptions across the different risk registers varies. There are examples of service risk registers (such as the Development and Place register) which provide a lengthy and detailed commentary of each risk to describe the cause and consequence of each documented risk. However, even within this register the quality of descriptions varies between risks. There are also examples of risk registers (such as the Environment register) with descriptions that are more basic and do not provide the reader with a proper understanding of the cause and consequence of the risk, and in some instances the commentary of these risks are copied and pasted across different risk titles. For example: • 'Failure to manage disabled facilities grants - With a budget of £900,000 to deliver improvements in residents houses using private contractors' • 'Failure to manage disabled facilities grants - This statutory function is required to protect the public when using facilities such as taxis, pubs and clubs and gambling establishments'

			• 'Failure to administer and maintain cemeteries correctly, whilst having due regard to religious faiths - Reputation risk to Council. Health risk to residents.' • 'Failure to provide parks and open spaces that are appropriately maintained - Reputation risk to Council. Health risk to residents.' This is also seen to a lesser extent in the corporate risk register which only records high level descriptions of each risk within the summary tab, with no further elaboration on the individual risk tabs. For example: • Failure to maintain financial integrity - Affecting the ability of the Council to meet its financial commitments in the longer term
2.3	Risks are assigned a category	×	Neither the service or corporate risk register categorise their risks (eg financial, regulatory, operational, staffing, etc.)
3.	**Risk Evaluation:**		
3.1	Risks are evaluated based on a defined scoring methodology	✓/×	The Council uses a standard 5x5 matrix to assess and score each risk. A detailed explanation on how to use the matrix is included as an appendix to the Risk Management Strategy and Framework including defined criteria for each rating in the matrix. However, there is one risk on the Communities and Leisure register which had no risk evaluation at the time of review.
3.2	Regular management challenge of the risk evaluations applied	✓	The maintenance of risk registers is led by the heads of service who will record and evaluate each identified risk. Where necessary the directors overseeing each service will provide input and challenge on the risk evaluations applied. When risk registers are updated each quarter the updates will also go to the SLT meeting where additional challenge will be applied. Where input is needed the Insurance and Risk Management Officer will also provide guidance and challenge on the process of evaluating risks.
3.4	The Council has identified key drivers of the identified risks	✓	The risk registers each include a column to record the key drivers of the risk. These are pre-defined drivers, for example the size of financial impact, service deliver impact, reputational impact, etc.
4.	**Assigning responsibilities for risk:**		
4.1	All risks have an owner	✓	All risks on the corporate and service registers have an owner assigned to oversee the management of the risk.

Assessment of maturity for this element					
	Naïve	Aware	Defined	Managed	Enabled
Current			✓		
Target				✓	

Risk Maturity Assessment – Risk Mitigation			
1.	**Current Mitigation:**	**✓/✗**	**Evaluation**
1.1	Responses to risks have been selected and implemented, having regard to the risk appetite.	✓/✗	Responses to risks are developed in order to bring them down to an acceptable level to the Council. All of the risk registers record the controls that have been implemented to mitigate the initial risk identified. The priority given to the treatment of a risk depends on its rating (consequence x likelihood). However, our review identified one risk on the Development and Place register and one risk on the Communities and Leisure register where the current risk score had remained constant when compared to the raw risk score. This was despite the register showing controls had been implemented to mitigate the risk indicating that in some instances there is insufficient actions being taken to mitigate the identified risks. We also found that across the risk registers the quality of descriptions of controls was not sufficient to provide the reader evidence that the risk was being managed effectively, with basic or generic controls being documented even for risks evaluated with a high raw risk.
2.	**Action Plans:**		
2.1	Action plans are in place for all risks that have not been accepted at the current level.	✗	Our review of the risk registers provided at the time of the audit found one instance (Risk PP6 on the Environment risk register) where no remedial actions had been documented despite the risk having not been mitigated to its target level. We also found that across all the risk registers provided, including the corporate risk register, the descriptions of the actions were inadequate to provide the reader with reasonable assurance that they would be sufficient to mitigate the risk, and would not be considered SMART actions. We also identified that across the service risk registers provided there were no implementation dates for the recorded actions and as such no assurance could be obtained that actions were being implemented in a timely manner. Additionally, not all actions on the corporate risk register had implementation dates, and where implementation dates were provided there was often significant delays in completing the actions, with several initial implementation dates more than three years old with the action still not having been implemented. For instance: • Risk 5 Action 2 – Initial completion date May 2018 and still incomplete • Risk 6 Action 4 – Initial completion date March 2018 and still incomplete

Assessment of maturity for this element					
	Naïve	Aware	Defined	Managed	Enabled
Current		✓			
Target				✓	

Risk Maturity Assessment – Reporting and Review			
1.	**Monitoring:**	**✓/✗**	**Evaluation**
1.1	A strategic risk register has been populated	✓/✗	The Council has documented a corporate risk register which documents the key strategic risks which could impact the Council realising its objectives as recorded in the Gedling Plan 2020 – 2023. However, as detailed above there are significant issues with the quality of the corporate risk register. These issues include: • Lack of quality in the description of the risk, the cause of the risk and consequence of the risk materialising • Actions that are insufficient to provide the reader with assurance that the risk will be mitigated to the target risk score • Actions recorded with no implementation date or implementation dates that have been slipping for three years or more • Actions where the quarterly update columns have not been consistently updated with progress towards implementation • Actions where the quarterly update has stated that the action is complete over the course of three or more updates, despite the register still showing the action as incomplete.
1.2	Departmental risk registers have been populated	✓/✗	Each of the services across the Council has its own local risk register that records the risks relevant to the service that could prevent the service from achieving its local objectives and that could have a wider impact of the achievement of the objectives in the Gedling Plan 2020 – 2023. However, as with the corporate risk register, there are a number of issues with the quality of these registers. These issues include: • The Development and Place risk register shows that for the past three quarters there has been no change in any of the risks facing the service in spite of the uncertain environment faced by organisations across the country, indicating there has not been sufficient consideration of risk within the service • Lack of quality in the description of the risk, the cause of the risk and consequence of the risk materialising • Actions that are insufficient to provide the reader with assurance that the risk will be mitigated to the target risk score • Actions recorded with no implementation date • A risk with no evaluation/scoring applied • Actions where the quarterly update columns have not been consistently updated with progress towards implementation • A risk where no actions had been recorded despite the risk not having been mitigated to its target score.
1.3	Risk registers are reviewed on a regular basis	✗	Council process requires that risk registers be reviewed on a quarterly basis, with updates recorded against each risk to indicate any changes which have occurred in the quarter.

			Our review found that across the three service risk registers dated April 2021 that were provided, only five out of 35 risks had progress updated in the March 2021 review column. Additionally, just 18/35 had progress updated provided in the December 2020 column and 23/35 in the September 2020 column. The corporate risk register was more consistent in providing quarterly updates in the summary tab with all risks having had their update recorded up to December 2020, although this was still not fully complete for the March 2021 update. However, the action progress recorded in the individual risk tabs was of a lower standard, where a simple statement such as 'in progress' was often recorded.
2.	**Reporting:**		
2.1	Regular reporting on key risks at corporate level	✓	The corporate risk register is subject to review on a quarterly basis at meetings of the SLT. A review of the risk register identified that these reviews are taking place and progress updates are recorded on the register. Additionally the minutes and reports of the SLT meetings show that the register is consistently being reported and discussed at these meetings on a quarterly basis.
2.2	Regular reporting on risks at division/department level	×	The update and review of the service risk registers is led locally by the heads of service with no local reporting mechanism in place. Risk management procedures require risk registers to be reviewed, updated and reported to the SLT on a quarterly basis and our interviews with the Insurance and Risk Management Officer and the heads of service indicated that these updates and reports occur on a consistent basis. However, as documented in 1.3 the evidence provided shows that the completion of these reviews is inconsistent and furthermore, the reports and minutes of SLT meetings provided as evidence for this review did not show reporting of service risk registers.
2.3	Decisions based on risk reports are fed back	✓/×	The Risk Management Strategy and Framework does not document any formal procedures for disseminating information or decisions down to services after registers are discussed at SLT. Our discussions with the heads of service indicated that there is no formal mechanism for this, but that risk registers are returned to the services after review and any feedback is provided verbally by the service director where necessary.
3.	**Assurance:**		
3.1	Assurance is provided on the effectiveness of the management of risks	×	The risk registers are formatted to record the controls in place to mitigate the recorded risks and the actions to be taken to further mitigate the risks to within the Council's risk appetite. However, there is no record made of the assurances the Council obtains that these controls are working effectively, or where there are gaps in assurance that need to be addressed. The Council should set out the assurances it has into the three lines of defence model: 1. Management control is the first line of defence in risk management

			2. The various risk control and compliance over- sight functions established by management are the second line of defence 3. Independent assurance is the third. This would be a more coordinated and robust approach to assessing the assurances in place and drawing on all the significant assurances the Council receives.

Assessment of maturity for this element					
	Naïve	Aware	Defined	Managed	Enabled
Current		✓			
Target				✓	

Risk Maturity Assessment – Continuous Improvement			
1.	**Continuous Improvement:**	**✓/✗**	**Evaluation**
1.1	The organisation's risk management approach and the Council's risk appetite are regularly reviewed and refined in light of new risk information reported	✓	There is no function within the current risk management structure to facilitate a formal review of the risk management function on a periodic basis. However, risk management is constantly under scrutiny within the organisation and has been highlighted as an increasingly important aspect of day to day operations over the past 15 months whilst the Council has been implementing its Covid-19 response. Where new information is presented which could impact the Council's management of risk, this is considered on a case by case basis and an appropriate response is implemented, taking in to consideration the risk appetite documented in the Risk Management Strategy and Framework.
2.	**KPIs:**		
2.1	KPIs are used to measure aspects of the risk management activity, e.g. timeliness of implementation of risk responses, number of risks materialising or surpassing impact-likelihood expectations •% of risk issues exceeding defined risk tolerance without action plans •Cycle time from discovery of a control deficiency to risk acceptance decision •% of staff having undertaken advanced risk management training.	✗	The Council does not monitor and report on any KPI's relating to risk management. Examples of possible indicators include: • % of risk issues exceeding defined risk tolerance without action plans • Cycle time from discovery of a control deficiency to risk acceptance decision • % of staff/members having formal risk management training.

Assessment of maturity for this element					
	Naïve	Aware	Defined	Managed	Enabled
Current			✓		
Target				✓	

STAFF INTERVIEWED

BDO LLP APPRECIATES THE TIME PROVIDED BY ALL THE INDIVIDUALS INVOLVED IN THIS REVIEW AND WOULD LIKE TO THANK THEM FOR THEIR ASSISTANCE AND COOPERATION.

Alison Ball	Director of Corporate Resources and Section 151 Officer
Alison Nicholson	Insurance and Risk Management Officer
Joelle Davies	Head of Regeneration and Welfare
Francesca Whyley	Head of Governance and Customer Services
David Archer	Head of HR, Performance and Service Planning
Lance Juby	Head of Communities and Leisure
Mike Avery	Head of Development and Place

APPENDIX I – ASESSMENT ACTION PLAN

The following table sets out the recommendations from our report. Where recommendations link across each of the five sections reviewed we have reported these together and cross referenced to the specific finding within the report. The table also includes the management comment arising from the recommendation, including the responsible officer and the expected implementation date. All recommendations are of medium priority unless otherwise stated.

Rec	Recommendation	Management Comment	Responsible Officer & Timescale
1.	Provide risk management training to all staff across the Council on a periodic basis as part of mandatory training cycles. The level of training should be proportional to the level of responsibility for risk management the officer/member holds. Heads of service and managers should be provided with comprehensive training to enable them to identify and adequately document a risk, identify appropriate mitigating controls and assurances and identify SMART actions to mitigate the risks. Officers below manager level should be provided with training to give them a sufficient understanding and appreciation of the importance of risk management and how it impacts their role. As a minimum, it should be every officer's responsibility to be aware of what risk is, to be able to identify factors that could indicate an increased level of risk that may need to be escalated to their manager and to report on this when it is identified. **(Risk Governance – Sections 2.1, 5.1, 5.2)**	Agreed. A tailored training programme will be developed for Officer and Members which is proportionate to the role and level of risk management responsibility. The frequency of training and timescales for future roll-out will be determined.	Head of Finance and ICT 31 March 2022

Rec	Recommendation	Management Comment	Responsible Officer & Timescale
2.	The roles and responsibilities section of the Risk Management Strategy and Framework (including Appendix 2) should be updated to ensure it includes the responsibility of officers below manager level within the risk management function. As a minimum their responsibilities should include the need to understand risk management and its importance to the organisation and to be able to identify risk factors that could indicate an increased level of risk and to report these to their managers. **(Risk Governance – Section 3.1)**	Agreed. A role of 'All Employees' to be added Roles and Responsibilities as part of the Risk Management Strategy reviewed. Responsibilities to be determined but may include: • To identify and report risk to their manager • To manage risk effectively within their job, implementing identified actions	Head of Finance and ICT 31 March 2022
3.	As a minimum all staff should have a general personal objective to support the management of risk within their service and their performance in delivering this objective should be evaluated as part of the appraisal process. (Low) **(Risk Governance – Section 3.2)**	This will be considered for those employees with specific responsibilities related to risk and recommendations will be made to Senior Leadership Team following consultation with the Head of HR, Performance and Service Planning	Head of Finance and ICT 31 March 2022
4.	The Risk Management Strategy and Framework should be reviewed and updated as necessary to ensure the information included is up to date and accurately reflects current procedure. It should also be updated to incorporate the recommendations raised in this review once implemented. Document control should also be added to the front cover of the Strategy to record who is responsible for managing the document and signing off changes, when the document was last updated, who approved the last update and a record of amendments to the document over time. **(Risk Governance – Section 7.1, 8.1)**	Agreed	Head of Finance and ICT 31 March 2022

Rec	Recommendation	Management Comment	Responsible Officer & Timescale
5.	The Risk Management Strategy and Framework should be updated to include enhanced guidance on the identification of risk, including specific methods that officers should use to ensure that all risks within their service have been identified and recorded within their risk register. **(Risk Assessment - Section 1.1)**	Further detail and examples to support risk identification are included in Appendix 6 of the existing risk management strategy. Further consideration of including additional methods of risk identification will be considered as part of the review of the Risk Management Strategy and Framework.	Head of Finance and ICT 31 March 2022
6.	The format of the risk registers should be updated to ensure that the risks identified are directly linked to the objectives in the Gedling Plan 2020 – 2023 and service plans which they impact. Risks should also be categorised by risk type within registers (such as financial, compliance, service delivery, etc.) to enable enhanced risk mapping to take place, giving the Council a better understanding of which areas it is exposed to the greatest risk. **(Risk Assessment - Section 2.1 and 2.3)**	Agreed	Head of Finance and ICT 31 March 2022
7.	All risk registers should be comprehensively reviewed, paying attention to the descriptions of risks. These should be updated and improved to ensure they sufficiently document the risk or hazard, its cause and the consequence should the risk materialise. **(Risk Assessment - Section 2.2)**	Agreed	Head of Finance and ICT 31 March 2022

Rec	Recommendation	Management Comment	Responsible Officer & Timescale
8.	All risks recorded on the risk register should be appropriately evaluated and assigned a risk score. **(Risk Assessment – Section 3.1)**	The detailed findings in this report show only one example where this has not been completed which perhaps demonstrates generally a good level of application of the methodology. Going forward, the quarterly review will include a check that risk evaluation and scoring has been completed.	Head of Finance and ICT 31 December 2021
9.	All risks within the corporate register should be accompanied by a direction of travel, which shows previous risk scores for at least the last three quarters to provide the reader with an understanding of whether the actions taking place are effectively mitigating the risk over time. **(Risk Mitigation – Section 1.1)**	Currently the direction of travel is indicated by a note within each quarterly review of the Corporate Risk Register and the quarterly Audit Committee Risk Scorecard clearly demonstrates direction of travel. Consideration will be given to improving the presentation to make this more transparent.	Head of Finance and ICT 31 December 2021
10.	Where a risk has been evaluated with a current risk score equal to its raw risk score despite controls in place and documented on the register, a further review should take place to identify why the current controls are ineffective and what can be done further to improve the effectiveness of these controls. **(Risk Mitigation – Section 1.1)**	Agreed. A review of the current risk registers will be completed to ensure full recording of controls and appropriate updating of the scores as controls are improved and implemented. Refresher training will be delivered as appropriate.	Head of Finance and ICT 31 December 2021

Rec	Recommendation	Management Comment	Responsible Officer & Timescale
11.	A comprehensive review of all registers should take place to improve the level of detail recorded for controls and action plans. All recorded controls should include narrative of how they mitigate the risk and all recorded actions should be SMART actions. Where an action has an implementation date that is overdue this should be raised with the risk owner to identify a specific plan to ensure the action is implemented in a timely manner with support from the SLT where needed. **(Risk Mitigation – Section 2.1)**	Agreed	Head of Finance and ICT 31 March 2022
12.	The format of the service risk registers should be updated to ensure they include implementation dates for each action on the register. **(Risk Mitigation – Section 2.1)**	Agreed	Head of Finance and ICT 31 December 2021
13.	The actions within the corporate risk register need to be reviewed to update the status of each action and ensure that the implementation status of the action accurately reflects the quarterly updates recorded. **(Risk Reporting and Review – Section 1.1 and 1.3)**	Agreed	Head of Finance and ICT 31 December 2021

Rec	Recommendation	Management Comment	Responsible Officer & Timescale
14.	The overall risk environment in the Development and Place service needs to be reviewed to ensure the service risk register still accurately reflects the service's exposure to risk due to the risk register currently showing no changes or updates to any of the risks for the past three quarters. **(Risk Reporting and Review – Section 1.2 and 1.3)**	Agreed. Discussion will be held with the Head of Service to identify any issues preventing completion and provide support to improve engagement.	Head of Finance and ICT 30 September 2021
15.	Where quarterly reviews of the risk registers take place the services must ensure that the update columns in the registers are updated to provide the reader with a sufficient understanding of what changes have taken place since the previous quarter. Where no changes have occurred an explanation of why this is the case should be recorded. **(Risk Reporting and Review – Section 1.2, 1.3, 2.1 and 2.2)**	Agreed. Heads of Service will be reminded of this requirement.	Head of Finance and ICT 30 September 2021
16.	The Risk Management Strategy and Framework should be updated to include the mechanisms in place to ensure discussions and decisions made at SLT meetings relating to the service risk registers are fed back to the relevant services in a timely manner. **(Risk Reporting and Review – Section 2.3)**	Agreed. Formal feedback from SLT will be provided to Heads of Service by the Head of Finance and ICT who attends SLT to present the quarterly review of the risk register.	Head of Finance and ICT 31 December 2021

Rec	Recommendation	Management Comment	Responsible Officer & Timescale
17.	Risk registers should be updated to record the assurances obtained that controls in place to manage risks are working effectively and where there are gaps in these assurances. This should follow the three lines of defence model. **(Risk Reporting and Review – Section 3.1)**	This will be considered as part of the review of the Risk Management Strategy and Framework.	Head of Finance and ICT 31 March 2022
18.	Once the other recommendations from the report have been implemented and embedded to improve the foundations of the Council's risk management function, KPIs should be used to measure the effectiveness of risk management activity at the Council. This can include the proportion of risks operating at the target level and/or the overall effectiveness of risk management (current risk versus target risk etc.). See Appendix II for a list of possible KPIs. **(Continuous Improvement – Section 2.1)**	Agreed. This will be included in the review of the Risk Management Strategy and Framework.	Head of Finance and ICT 31 March 2022

APPENDIX II – EXAMPLE KPIs

- Timeliness of implementation of risk responses
- Percentage of risks operating at the target level
- The overall effectiveness of risk management (current risk versus target risk)
- Number of risks materialising or surpassing impact-likelihood expectations
- % of risk issues exceeding defined risk tolerance without action plans
- Cycle time from discovery of a control deficiency to risk acceptance decision
- % of staff having undertaken risk management training
- Heads of Service must attend at least 75% of the XXX Council/Committee meetings and departmental governance group meetings and ensure that a designated deputy attends in their absence

APPENDIX III - RISK MATURITY ASSESSMENT MATRIX

	Risk Governance	Risk Identification and Assessment	Risk Mitigation and Treatment	Risk Reporting and Review	Continuous Improvement
Enabled	Risk management and internal control is fully embedded into operations. All parties play their part and have a share of accountability for managing risk in line with their responsibility for the achievement of objectives.	There are processes for identifying and assessing risks and opportunities on a continuous basis. Risks are assessed to ensure consensus about the appropriate level of control, monitoring and reporting to carry out. Risk information is documented in a risk register.	Responses to the risks have been selected and implemented. There are processes for evaluating risks and responses implemented. The level of residual risk after applying mitigation techniques is accepted by the organisation, or further mitigations have been planned.	High quality, accurate and timely information is available to operational management and directors. The Audit Committee reviews the risk management strategy, policy and approach on a regular basis, e.g. annually, and reviews key risks, emergent and new risks, and action plans on a regular basis, e.g. quarterly.	The organisational performance management framework and reward structure drives improvements in risk management. Risk management is a management competency. Management assurance is provided on the effectiveness of their risk management on a regular basis.
Managed	Risk management objectives are defined and management are trained in risk management techniques. Risk management is written into the performance expectations of managers. Management and executive level responsibilities for key risks have been allocated.	There are clear links between objectives and risks at all levels. Risk information is documented in a risk register. The organisation's risk appetite is used in the scoring system for assessing risks. All significant projects are routinely assessed for risk.	There is clarity over the risk level that is accepted within the organisation's risk appetite. Risk responses appropriate to satisfy the risk appetite of the organisation have been selected and implemented.	The Audit Committee reviews key risks, emergent and new risks, and action plans on a regular basis, e.g. quarterly. It reviews the risk management strategy, policy and approach on a regular basis, e.g. annually. Directors require interim updates from delegated managers on individual risks which they have personal responsibility.	The organisation's risk management approach and the Council's risk appetite are regularly reviewed and refined in light of new risk information reported. Management assurance is provided on the effectiveness of their risk management on an ad hoc basis. The resources used in risk management become quantifiably cost effective. KPIs are set to improve certain aspects of the risk management activity, e.g. timeliness of implementation of risk responses, number of risks materialising or surpassing impact-likelihood expectations.

Defined	A risk strategy and policies are in place and communicated. The level of risk-taking that the organisation will accept is defined and understood in some parts of the organisation, and it is used to consider the most appropriate responses to the management of identified risks. Management and executive level responsibilities for key risks have been allocated.	There are processes for identifying and assessing risks and opportunities in some parts of the organisation but not consistently applied in all. All risks identified have been assessed with a defined scoring system. Risk information is brought together for some parts of the organisation. Most projects are assessed for risk.	Management in some parts of the organisation are familiar with, and able to distinguish between, the different options available in responding to risks to select the best response in the interest of the organisation.	Management have set up methods to monitor the proper operation of key processes, responses, and action plans. Management report risks to directors where responses have not managed the risks to a level acceptable to the Council.	The Council gets minimal assurance on the effectiveness of risk management.
Aware	There is a scattered, silo-based approach to risk management. The vision, commitment and ownership of risk management have been documented. However, the organisation is reliant on a few key people for the knowledge, skills and the practice of risk management activities on a day-to-day basis.	A limited number of managers are trained in risk management techniques. There are processes for identifying and assessing risks and opportunities, but these are not fully comprehensive or implemented. There is no consistent scoring system for assessing risks. Risk information is not fully documented.	Some responses to the risks have been selected and implemented by management according to their own perception of risk appetite in the absence of a Council-approved appetite for risk.	There are some monitoring processes and ad hoc reviews by some managers on risk management activities.	Management does not assure the Council on the effectiveness of risk management.
Naive	No formal approach developed for risk management. No formal consideration of risks to business objectives, or clear ownership, accountability and responsibility for the management of key risks.	Processes for identifying and evaluating risks and responses are not defined. Risks have not been identified nor collated. There is no consistent scoring system for assessing risks.	Responses to the risks have not been designed or implemented.	There are no monitoring processes or regular reviews of risk management.	Management does not assure the Council on the effectiveness of risk management.

APPENDIX IV – TERMS OF REFERENCE

BACKGROUND

The risk management process involves the identification, evaluation and treatment of risk as part of a continuous process aimed at helping the Council and individuals reduce the incidence and impacts of risks that they face.

Risk management is therefore a fundamental part of both the operational and strategic thinking of every part of the service delivery within the organisation. This includes, corporate, business and financial risks.

At Gedling Borough Council ('the Council'), a Risk Management Strategy and Framework was approved by the Cabinet in October 2017, which provides guidance on the processes, procedures, roles and responsibilities for risk, and sets out the context on how risks are to be managed.

The Corporate Risk Register is a key enabler of the Strategy and Framework, and provides assurance on the key risks identified as corporate risks. The Corporate Risk Register is reviewed on a quarterly basis by the Senior Leadership Team and the Audit Committee.

A monitoring report is provided by the Director of Corporate Resources and Section 151 Officer to the Audit Committee.

PURPOSE OF REVIEW

The purpose of the BDO Risk Maturity Assessment is to help ensure an effective risk management culture becomes embedded across the Council, by highlighting areas where processes could be improved. As primarily an advisory piece of work assessing the Council's current position against the BDO Risk Maturity Matrix, this assessment will not generate an assurance opinion.

KEY RISKS

Based upon the risk assessment undertaken during the development of the internal audit operational plan, through discussions with management, and our collective audit knowledge and understanding the potential key risks areas to be reviewed are:

- There is not a clear understanding of risk within the Council
- The risks on the risk registers do not correspond to those actually facing the Council
- Risks are not reviewed on a regular basis and appropriate assurance and controls assigned to them
- Escalation and management review of risks is insufficient, and mitigating actions are ineffective.

SCOPE OF REVIEW

The Risk Maturity Assessment will cover the following elements of risk management:

- Governance
- Identification and assessment
- Mitigation and treatment
- Reporting and review
- Continuous improvement.

Based on documentary review and interviews with key staff, each element will be judged on a five-part scale between 'naïve' and 'enabled', as outlined in the BDO Risk Maturity matrix in Appendix 2.

However, Internal Audit will bring to the attention of management any points relating to other areas that come to their attention during the course of the audit. We assume for the purposes of estimating the number of days of audit work that there is one control environment, and that we will be providing assurance over controls in this environment. If this is not the case, our estimate of audit days may not be accurate.

APPROACH

Our approach will be to conduct interviews and perform documentary review to establish the level of maturity of each of the key elements of risk management considered by the assessment.

With social distancing measures affecting everyone, this review will be undertaken remotely with communications via email and video conferencing. We appreciate that your staff may have other priorities during the COVID-19 pandemic and we will work with them to accommodate convenient times to discuss documentation provided.

ADDED VALUE

The review will enable us to benchmark the Council's risk maturity level against other local government organisations both locally and nationally.

FOR MORE INFORMATION:

Greg Rubins

Greg.Rubins@bdo.co.uk