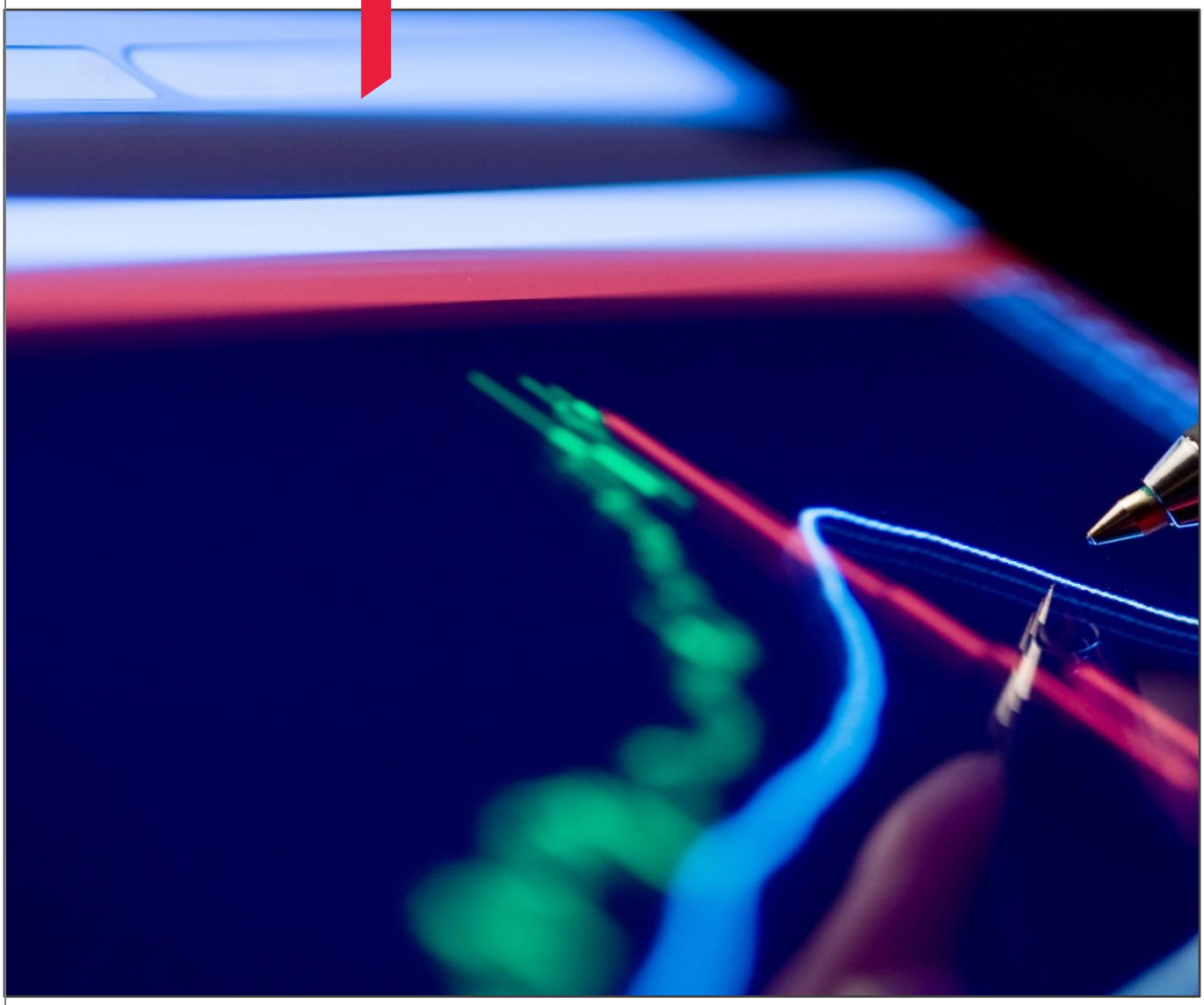

MALDON DISTRICT COUNCIL

INTERNAL AUDIT REPORT

RISK MATURITY
JUNE 2022

IDEAS | PEOPLE | TRUST

BDO

CONTENTS

EXECUTIVE SUMMARY 87
ASSESSMENT OF RISK MATURITY AGAINST THE BDO RISK MATURITY MODEL.... 90
APPENDIX I – EXAMPLE KPIS 100
APPENDIX II – RISK EVALUATION GUIDANCE 101
APPENDIX III – RISK MATURITY ASSESSMENT MATRIX 102
APPENDIX IV – TERMS OF REFERENCE 104

DISTRIBUTION	
Cheryl Hughes	Programmes, Performance and Governance Manager
Eloise Howard	Specialist - Performance

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.

REPORT STATUS	
Auditors:	James Savigar
Dates work performed:	03 May 2022 – 23 June 2022
Draft report issued:	28 June 2022
Final report issued:	5 July 2022

EXECUTIVE SUMMARY

SCOPE

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. The previous review, completed in 2019, placed the Council as Aware or Defined across the five areas included in the scope.

AREAS REVIEWED

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	Managed	Defined	Aware	Defined	Managed
Target	Enabled	Enabled	Defined	Enabled	Enabled

When the previous review was conducted in 2019, the current and target maturity assessments were:

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

AREAS OF STRENGTH

- There is a robust system in place to ensure the corporate risk register is updated and subject to review at least every quarter by senior leadership and members.
- The SharePoint system allows officers to easily raise concerns to be considered for addition to the risk register.
- The SharePoint system allows for good visibility of risks recorded on the corporate risk register.
- The SharePoint system provides automated reminders to risk owners to ensure updates to the risk register are completed in a timely manner.
- The Council's risk management process and system is subject to regular review to consider where improvements to processes can be made.
- There is a clear systematic approach for how risks should be managed which is clearly communicated within the Risk Management Policy.

AREAS OF CONCERN

- Whilst risks recorded on the corporate risk register are linked to strategic objectives, no risk mapping takes place to clearly illustrate the objectives that are exposed to the greatest risk, which can be included in risk reports to the Performance, Governance and Audit Committee.
- The approach for describing risks as set out in the Risk Management Policy is not consistently applied to risks on the corporate risk register, where risk descriptions do not clearly and succinctly set out the risk, cause and consequence.
- Whilst the Risk Management Policy provides some guidance on how to apply the risk evaluation matrix, by defining the likelihood scores from unlikely to definite and the impact scores from negligible to major, there is no detailed guidance on the specific definition of these terms, increasing the likelihood that risks will be evaluated inconsistently.
- Mitigating actions are not consistently identified to address risks recorded on the corporate risk register which have not been mitigated to beneath the tolerance threshold. There is also no system in place to monitor the implementation of the actions that have been documented.
- Although risks are identified in Manager's service plans, there is no standard process in place for the review and reporting of local risks recorded within service plans, with each service taking a different approach.

CONCLUSION

- The Council scores above average against the key indicators included within the report when compared to other Councils, as evidenced in the graph below. Whilst this indicates that overall the Council's systems for risk management are operating effectively, there are still improvements that can be made to more effectively manage risk across the Council, particularly within services, where there is less structure with regards to risk management. Since our review in 2019, the Council has improved its level of maturity in all areas, except for risk mitigation, which has fallen from defined to aware over the period, largely due to the inconsistent documentation of mitigating actions on the corporate risk register and the absence of a systematic process for monitoring the implementation of actions that are recorded. If this issue is addressed, and ongoing efforts to improve the risk management function continue by implementing the recorded actions, the Council will meet the target maturity level and align with best practice for risk management.

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 developed a Corporate Plan for 2021 -2023. It is divided into four main areas; Place, Prosperity and Community and Performance and Value under which sit 19 outcomes. Alongside this the plan also incorporates eight core values: • Have a customer focus • Be respectful to others • Act ethically and with integrity • Be innovative • Collaborate to deliver • Be accountable for our actions • Be open and transparent • Be ambitious
1.2	Division / department objectives are set and linked to the organisation's objectives.	✓	Each area has its own service plan which is developed between the service director and manager. The service plan incorporates the key objectives the service is aiming to achieve for the year, linking back to the four main areas in the Corporate Plan.
2.	**Tone at the top**		
2.1	The Board have mandated that a formal approach be taken to risk management and set out why risk management is important.	✓	The Council has a Risk Management Policy which documents a clear step by step approach for risk management, as follows: 1. Identify Corporate, Service, Project or Partnership Objectives 2. Identify Risks 3. Assess adequacy of existing controls 4. Assess Inherent Risk Level 5. Identify further mitigating actions required 6. Monitor impact of mitigating actions on residual risk 7. Review and report The policy also sets out the roles and responsibilities of staff to fulfil this approach.
3.	**Roles and responsibilities:**		
3.1	Roles and responsibilities for risk management have been defined centrally and across divisions and departments.	✓	Roles and responsibilities for risk management are defined within the Risk Management Policy under the following categories: • Full Council • Performance, Governance and Audit Committee • Corporate Leadership Team • Risk owners • Managers • All staff

3.2	Effectiveness in discharging risk management responsibilities is evaluated as part of individual performance review/appraisal.	✗	From our interviews with the corporate risk team and service plan owners, we found that whilst there were ongoing conversations with risk owners to determine how effectively their risks were being mitigated, this did not represent a systematic performance appraisal process where objectives are set and progress formally reviewed and documented.
4.	**Resources:**		
4.1	Resource requirements have been identified and budget allocated.	✓	The Council has developed a dedicated SharePoint risk register system for the documentation, monitoring and reporting of risk. This process is managed by the Performance Specialist, with oversight from the Programmes, Performance and Governance Manager.
4.2	Regular review takes place of ongoing resource requirements.	✓	Through interviews with the Performance Specialist, we found that the Council is continually reviewing its SharePoint system to improve functionality.
5.	**Training:**		
5.1	Training undertaken for managers and staff responsible for risk management.	✓/✗	There is a risk management presentation which is available for all staff and included as part of the induction pack for new staff. The presentation is also available on the intranet for staff to view if they need to refresh their knowledge of the content. There is no dedicated training programme for managers or those with additional risk management responsibilities. The Risk Management Policy is due to be updated in November 2022, at which point the training will also be updated.
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 board at corporate level	✓	The Risk Management Policy includes a section which communicates a brief risk appetite statement. However, it also complements this with additional narrative throughout the policy, including where guidance is provided on the risk scoring matrix, which indicates the level of risk that is tolerable before it must be escalated for management/director consideration
6.2	Risk appetite statements are in place and within departments.	✓	There are no dedicated risk appetite statements for departments. However, the central Risk Management Policy is expected to be applied consistently across all departments, and as such they are expected to apply the central risk appetite statement when managing risks.
7.	**Risk policy:**		

7.1	A risk management policy is in place and has been communicated throughout the organisation.	✓	The Council has a Risk Management Policy that was last updated in November 2019 and approved by the Performance, Governance and Audit Committee. The policy is next due for review in November 2022.

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

Recommendations for improvement - Governance

1. A systematic process for reviewing how effectively officers are discharging their risk management responsibilities should be implemented. This should include ensuring all individuals with risk management responsibilities have specific objectives captured via the appraisal process, with these being subject to regular review throughout the year, by analysing the risks the individual is responsible for on the risk register and reviewing how effectively they are being mitigated.
2. Whilst basic risk management training should be issued to all staff across the Council, enhanced risk management training should be mandatory for all officers with specific risk management responsibilities, which should be completed on a rolling 3 yearly cycle to ensure they maintain the skills necessary to effectively mitigate risk.

Management Response	Responsibility and Implementation Date	
1. We will look into how we report individual risk management as part of the framework update. 2. This is already in keeping with what we have done and we can continue to work to a three year training cycle in the policy update.	Responsible Individual:	1. Cheryl Hughes 2. Cheryl Hughes
	Implementation Date:	1. November 2022 2. November 2022

Risk Maturity Assessment – Risk Assessment			
1.	**Risk Identification:**	**✓/×**	**Evaluation**
1.1	Comprehensive process in place for systematically identifying risks throughout the organisation.	✓	There is an annual process across services where service management engage with the service director and officers to identify objectives for the year and document these on their service plan. Risks which could impact the achievement of these objectives are identified and also documented within the service plan. All risks are scored and any which are above the threshold must be considered for inclusion on the corporate risk register via SharePoint. Officers are responsible for staying alert to emerging risks whilst discharging their duties throughout each year. If an officer believes they have identified a risk, they must complete a risk report via the SharePoint system, following which it is considered for inclusion on to the corporate register.
2.	**Risk Analysis:**		
2.1	Risks are linked to objectives.	✓/×	When risks are added to the corporate register they are linked to the area of the corporate plan that they relate to (Place, Prosperity and Community and Performance and Value) and the strategic objective which they could impact on. However, whilst risks are linked to objectives, this information is not used to produce risk maps to better understand the Council's exposure to risk in different areas.
2.2	Risks are clearly described.	×	There is a section in the Risk Management Policy where detailed guidance is provided on how to document and describe a risk using a description, cause, consequence format. However, on review of the risk register, this is not being applied to the risk descriptions, which provide basic descriptions without clearly setting out the cause and consequence aspects. For example, R8 on the corporate risk register states 'Failure to meet the affordable housing need.' This does not provide any information to the reader on the root cause of this risk and the consequences should the risk materialise. On certain risks, this additional detail is included to some degree in the risk commentary. However, the commentary section is largely used to record updates to the risk, making it difficult to identify a more detailed description of the risk within the commentary.
2.3	Risks are assigned a category.	✓	The Risk Management Policy sets out different categories of risk which are built in to the SharePoint system which are applied to risks when they are added to the corporate risk register. We observed that all risks were assigned one of the following categories: • Compliance • Financial • Operational • Strategic
3.	**Risk Evaluation:**		

3.1	Risks are evaluated based on a defined scoring methodology.	✓/×	The Risk Management Policy includes a standard 5x5 matrix of likelihood vs impact which is applied to the assessment of all risks added to the corporate risk register and local service plans. However, whilst the Risk Management Policy provides some guidance on how to apply the risk evaluation matrix, by defining the likelihood scores from unlikely to definite and the impact scores from negligible to major, there is no detailed guidance on the specific definition of these terms, increasing the likelihood that risks will be evaluated inconsistently. An example of how this guidance could be expanded is attached at appendix II
3.2	Regular management challenge of the risk evaluations applied.	✓	All new risks submitted via the SharePoint system are first subject to review by the Performance Specialist. These risks are then added to the risk report made to the Quarterly Risk and Performance Clinic for consideration and challenge of the ratings where appropriate.
4.	**Assigning responsibilities for risk:**		
4.1	All risks have an owner.	✓	At the time of our audit there were 17 risks on the corporate risk register, all of which were assigned a risk owner. All service plans are owned by the relevant service manager and director, so all risks are owned locally.

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

Recommendations for improvement - Risk Assessment

1. A risk map should be produced to enable the Council to better understand the areas to which it is exposed to the greatest risk. The risk map should plot each risk and its overall risk score against the different strategic objectives to see which of these are exposed to the greatest risk, enabling the Council to better prioritise interventions.
2. All risks on the corporate risk register should be subject to an enhanced one off review to determine whether their description meets the requirements of the Risk Management Policy by including the event/hazard, cause and consequence. This should be captured in the risk title so that it is pulled through to reports made to the Performance, Governance and Audit Committee. For example, R8 'Failure to meet the affordable housing need' could be amended to (the cause and consequence included below are for illustrative purposes only on how to properly record a risk on the risk register, and are not intended to imply what the actual cause and consequence are):

   Event/Hazard

   The Council will fail to meet the needs of the community for affordable housing.

   Cause

   Developers are more frequently paying commuted sums to the Council as opposed to including affordable housing within developments, with it being increasingly difficult to use the sums to secure more affordable housing due to the lack of land supply for housing.

   Consequence

Failure to meet affordable housing needs could result in an increased level of homelessness across the borough 3. Additional guidance on how to apply the different likelihood and consequence risk scores should be added to the Risk Management Policy to improve the consistency of scoring on the register.	
Management Response	**Responsibility and Implementation Date**
1. We will look in to reporting at this level as part of the balance scorecard. 2. We will complete this exercise as part of the launch of the new framework. 3. This will be further enhanced as part of the framework update.	Responsible Individual: 1. Eloise Howard 2. Paul Dodson 3. Cheryl Hughes Implementation Date: 1. March 2023 2. March 2023 3. November 2022

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.	✓/×	For all 17 risks documented on the corporate risk register, controls have been identified to mitigate the inherent risk. However, not all controls have been successful in mitigating risks over time where current risk scores exceed inherent risk scores. Controls to mitigate risks identified on local service plans are recorded in the comments/mitigating actions section.
2.	**Action Plans:**		
2.1	Action plans are in place for all risks that have not been accepted at the current level.	×	Within the SharePoint system there is a register separate to where risks are documented to capture mitigating actions. These are linked back to the individual risks on the risk register. Our review of the 17 risks on the register found that actions were only documented against eight. Furthermore, our interviews with the Performance Specialist found that there is currently no embedded process for reviewing and monitoring the implementation of actions recorded against risk. There are mitigating actions captured against risks on local service plans. However, these are largely only simple statements and are not SMART actions, such as within the 'Strategy, Policy, Communications and Commercial' and 'Resources' service plans, where example actions include 'Learn from feedback on failed bids' and 'Regular monitoring of requirements, risks and progress'. There is also no process for documenting progress towards implementing these actions.

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

Recommendations for improvement – Risk Mitigation	
For all risks where current controls are not successfully reducing the risk score to within the Council's risk appetite, mitigating actions should be identified to further strengthen the controls. These mitigating actions should be documented within the SharePoint system and allocated an owner and implementation date. These actions should be monitored on an ongoing basis, and action owners should be required to provide updates on progress alongside the process for updating risk registers. These actions should be reported to Risk and Performance Clinic and Performance, Governance and Audit Committee for discussion and oversight.	
Management Response	Responsibility and Implementation Date
As part of strategy and reporting update, we will look to enhance tracking of the mitigating actions and include their performance monitoring as part of wider performance reporting.	Responsible Individual: Eloise Howard Implementation Date: January 2023

Risk Maturity Assessment – Reporting and Review			
1.	**Monitoring:**	**✓/✗**	**Evaluation**
1.1	A strategic risk register has been populated.	✓	A corporate risk register is maintained using SharePoint which is subject to regular update and review on a quarterly basis.
1.2	Departmental risk registers have been populated.	✓/✗	Departments across the Council do not have dedicated local risk registers. Risks which are of a low significance and therefore not required to be escalated to the corporate risk register are captured on the departmental service plans. However, as these are not full risk registers, the information recorded is limited to just a risk description, score and mitigating action.
1.3	Risk registers are reviewed on a regular basis.	✓/✗	The SharePoint system that is used to maintain the corporate risk register sends notifications to risk owners when risks are required to be reviewed and updated. These updates are initially checked by the Performance Specialist to confirm risks are updated in a timely manner prior to reporting taking place. The Risk Management Policy requires owners of service plans to manage their risks on an ongoing basis. However, it does not provide detailed guidance on the minimum expectations for how this responsibility should be discharged. Our interviews with owners of service plans found that this has resulted in different approaches being taken to reviewing risks on service plans, with some monitoring theirs on a weekly basis, whilst another conducted bi-monthly reviews.
2.	**Reporting:**		
2.1	Regular reporting on key risks at corporate level.	✓	The corporate risk is reported at the Quarterly Risk and Performance Clinic and at Quarterly Performance, Governance and Audit Committee.
2.2	Regular reporting on risks at division/department level.	✗	As in 1.3, whilst the Risk Management Policy places responsibility for managing local risks on service plan owners, there are no documented processes in place for the reporting of risks at service level.
2.3	Decisions based on risk reports are fed back.	✓/✗	The corporate risk register is subject to a systematic reporting process, with feedback on discussions being provided back to risk owners. However, due to their being no robust and consistent reporting process in place across all departments and services, there is only limited feedback available on local service risks.
3.	**Assurance:**		

3.1	Assurance is provided on the effectiveness of the management of risks.	✓/×	Due to the robust review and reporting system in place for monitoring risks on the corporate risk register there is good oversight of risk at this level. However, due to the lack of structure around the management of risk at departmental level, only limited assurance can be provided that these are being effectively managed.

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

Recommendations for improvement - Reporting and Review

The process for reviewing and reporting local risks within departmental service plans should be standardised by setting a minimum expectation within the Risk Management Policy which departmental managers should be required to meet. This should include the minimum frequency at which risks within service plans should be reviewed, who should be involved in completing these reviews, and where updates to risks within service plans should be reported.

Management Response	Responsibility and Implementation Date	
This will be specified in the updated risk management framework.	Responsible Individual:	Cheryl Hughes
	Implementation Date:	November 2022

Risk Maturity Assessment - Continuous Improvement			
1.	**Continuous Improvement:**	**✓/✗**	**Evaluation**
1.1	The organisation's risk management approach and the Board's risk appetite are regularly reviewed and refined in light of new risk information reported.	✓	The Council's Risk Management Policy is subject to routine review every three years. However, between these reviews the process is continually considered for improvements, with the Performance Specialist working with the Programmes, Performance and Governance Manager and the Risk and Performance Clinic to identify areas where the system can be improved.
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 uses a balanced scorecard to monitor a range of KPIs. One of these KPIs relates to corporate risk tolerance, where risks on the corporate risk register are categorised as below tolerance or amber, yellow or red tolerance. However, there are no definitions of what these terms mean on the report, and no indication of what would be required to meet the requirements of the KPI. Furthermore, there are no other KPIs included, relating to other areas such as consistency of mitigating actions being recorded on the corporate risk register.

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

Recommendations for improvement - Continuous Improvement

The Council should expand its suite of KPIs for risk management, and ensure all indicators are defined, including what is required to be within the tolerance of the KPI. See Appendix I for example KPIs that should be considered for implementation.

Management Response	Responsibility and Implementation Date
We will consider this and add into the wider balance scorecard reporting as part of the new strategy launch.	Responsible Individual: Eloise Howard
	Implementation Date: March 2023

APPENDIX I – 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
- SMT must attend at least 50% of the XXX governance meetings
- Heads of Departments 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 II – RISK EVALUATION GUIDANCE

IMPACT			
Score	Finance	Service	Reputation
1	Less than £10,000	No or very little impact on services.	Some negative publicity.
2	£10,000 to £50,000	Disruption of services causing inconvenience. May cause efficiency/effectiveness problems.	Regular negative publicity.
3	£50,000 to £500,000	Loss of service for a significant period (less than a month).	Loss of public confidence, protest action.
4	£500,000 to £3.5m	Loss of services to such an extent that effects on the community will be measurable.	Punitive action by reguators requiring significant organisational changes.
5	£3.5m plus	Permanent loss of a significant service. Threatens the viability of the organisation.	Damage to such an extent that the organisation must cease to exist as it.

LIKELIHOOD					
Score	1	2	3	4	5
Definition	Could happen, but probably never will.	Not likely to occur under normal circumstances.	May occur at some time.	Expected to occur at some time.	Expected to occur regularly under normal circumstances or a single irreparable occurrence.

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 board 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 board 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 Board'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 board.	The Board 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 board-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 Board 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 Board on the effectiveness of risk management.

APPENDIX IV - TERMS OF REFERENCE

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 associated with the area under review 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 & APPROACH

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 1.

The scope of the review is limited to the areas documented under the scope and approach. All other areas are considered outside of the scope of this review. 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.

It is intended that this audit will be completed through a combination of remote working and onsite meetings and testing, based upon the most effective way of carrying out the work.

In delivering this review BDO may need to observe and test confidential or personal identifiable data to ascertain the effective operation of controls in place. The organisation shall only provide the Shared Personal Data to BDO using secure methods as agreed between the parties. BDO will utilise the data in line with the General Data Protection Regulations 2016 (GDPR) and the Data Protection Act 1998, and shall only share Personal Data on an anonymised basis and only where necessary.

FOR MORE INFORMATION:

GREG RUBINS

greg.rubins@bdo.co.uk

www.bdo.co.uk