MALDON DISTRICT COUNCIL

INTERNAL AUDIT REPORT

RISK MANAGEMENT

JULY 2019

BDO

EXECUTIVE SUMMARY..... 2

ASSESSMENT OF RISK MATURITY AGAINST THE BDO RISK MATURITY MODEL..... 5

APPENDIX I – EXAMPLE KPIs..... 14

APPPENDIX II -EXAMPLE RISK APPETITE STATEMENT..... 15

APPPENDIX III -EXAMPLE RISK DEFINITION GUIDANCE.....16

APPENDIX IV – RISK MATURITY ASSESSMENT MATRIX.....17

APPPENDIX V -TERMS OF REFERENCE.....19

Distribution	
Name	Job Title
Cheryl Hughes	Programmes, Performance and Governance Manager
Paul Dodson	Director of Strategy, Performance and Governance

Report Status list	
Auditors:	Chris Andre
Dates work performed:	17/06/19 – 02/07/19
Draft report issued:	05 July 2019
Final report issued:	24 July 2019

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 'risk enabled' status.

The Council is currently undertaking an extensive project that has significantly altered the structure and working practices within the Council and has resulted in a large turnover of staff. This includes the key risk management position within the Council, which now falls under the newly appointed Programmes, Performance and Governance Manager.

The Risk Management Policy states it is for all staff to be involved within the Risk Management process with risks to be reviewed at service level and escalated to the Corporate Risk Register (CRR) if scoring hits a certain threshold. The Corporate Leadership Team (CLT), with Audit Committee also having oversight, monitor corporate risks whilst service level risks are to be monitored by the service managers.

Officers informed us that the Council, in its past, has generally been risk adverse with a hierarchical, centralised structure resulting in only executive management having responsibility for risk. However, with the work currently underway it is seen as a turning point with the move to a more de-centralised structure allowing for the risk management process to be further embedded at all levels of the Council, promoting a bottom-up approach with regards to risk identification and involvement.

The Council is well positioned to improve on the maturity scoring stated below, with steps already in place to advance and replace processes and systems to make them fit for purpose given the changes underway. There is already good buy-in from the three Directors who understand the need for strong risk management and are proactive in embedding it further. It is anticipated that a follow up of this audit next year would identify much improved results.

GOOD PRACTICE:

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

- Quarterly updates of all mitigating actions are undertaken with TEN (Council's risk management system) issuing email reminders to the owners of the actions – NB, this system is due to be replaced by one with greater functionality
- Risk Management training for Members has recently been undertaken to ensure a better understanding of their role whilst induction training is being improved to embed Maldon's specific identification and management processes
- A Corporate Risk Register is in place which is monitored and reviewed with risk scoring changed where necessary
- Steps to replace the risk management system are already well underway to allow for improved reporting

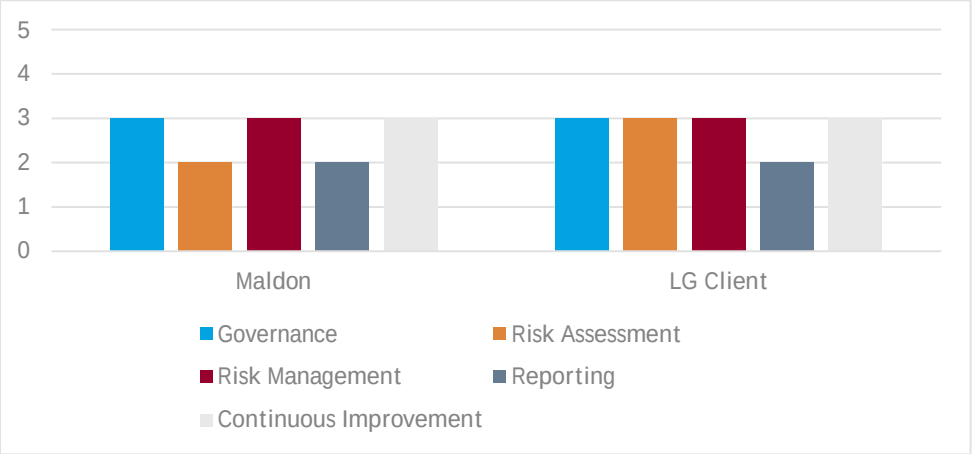
KEY FINDINGS

Recommendations have been raised against each of the areas of the risk maturity assessment. However, our key findings are:

- Inconsistent practices with regard to the identification and ongoing monitoring of risks at service level
- Mitigating actions are not always appropriate or specific enough to ensure progress against reducing the risk
- The Council does not currently report on any KPIs relating to their management of risk
- Not all risks at service level are required to have mitigating actions established and continually monitored

Having conducted a risk assessment at another district council recently it can be seen that both scored similarly. This is evidenced by the graph below:

1 – Naïve
2 – Aware
3 – Define
4 – Managed
5 – Enabled



OVERVIEW

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 I 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.

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

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 recently developed a new Corporate Plan running from 2019 -2023. It is divided into three main areas; Place, Community and Prosperity, under which sit 32 objectives.
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 holds a Risk Management Policy which states that it is the responsibility for all staff to: Report hazards and risks to their Managers, undertake their duties within risk management guidelines, Health and Safety Risks are to be dealt with immediately - where possible the risk should be removed or eliminated, otherwise it must be reported as a matter of urgency and steps taken to warn people of the problem
3.	**Roles and responsibilities:**		
3.1	Roles and responsibilities for risk management have been defined centrally and across divisions and departments.	✓	Roles and responsibilities are set out within the Council's Risk Management Policy at section 4 and includes Full Council, Finance and Corporate Services Committee, Audit Committee, CLT, Risk Owners, Managers and All Staff.
3.2	Effectiveness in discharging risk management responsibilities is evaluated as part of individual performance review/appraisal.	✗	From our discussions with staff within the Council, we identified that the effectiveness of risk management was not consistently incorporated into individuals performance appraisals
4.	**Resources:**		
4.1	Resource requirements have been identified and budget allocated.	✓	The Programmes, Performance and Governance Manager is the central contact and main individual responsible for risk management within the Council. The Council also utilises TEN, which is used as a repository for risks on the corporate risk register and their respective mitigating actions. The system is due to be replaced.

4.2	Regular review takes place of ongoing resource requirements.	✓	The Programmes, Performance and Governance Manager was recently appointed following the review of the Councils structure. The current risk management software has limited capability and therefore steps are already underway to replace it with software with much improved reporting and analytical capabilities
5.	**Training:**		
5.1	Training undertaken for managers and staff responsible for risk management.	✓	A Risk Management Workshop was recently undertaken to ensure that Members understand their roles and responsibilities
5.2	Training in risk management is provided to all staff.	✓/×	The induction training includes a section on risk management, albeit brief. However, it is positive to note that this is due to be improved with training in relation to risk management and risk mitigation being configured and will be completed via e-learning. However, some of the managers spoken to had not received any recent risk management training.
6.	**Risk Appetite:**		
6.1	A formal risk appetite statement has been agreed by the board at corporate level	✓/×	The Risk Management Policy discusses the Council's risk appetite in terms of the scoring for a risk as well as in more detail as part of their thematic strategy, however, there is no formal Risk Appetite Statement. See Appendix II for an example risk appetite statement.
7.	**Risk policy:**		
7.1	A risk management policy is in place and has been communicated throughout the organisation.	✓	A Risk Management Policy is in place, was reviewed in 2017 and is due to be reviewed again in 2020. However, due to the significant changes within the Council and change in structure, the policy is to be reviewed before 2020.

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

Recommendations for improvement – GOVERNANCE
1. Risks should be linked to the corporate objectives of the Council 2. Those with risk management responsibilities should have this area of their job role reviewed during annual appraisals 3. Service Level Managers should be provided with refresher training to ensure a consistent approach to risk management across the Council 4. Consideration should be given to establishing a formal risk appetite statement for the Council, which is reviewed on an annual basis with the Audit Committee. This will help to embed a risk aware culture and ensure a consistent reflection on the direction of risk management within the Council

Management Response	Responsibility and Implementation Date
½. We have created a new template for SMART appraisals which links their role to the corporate objectives and have a question in there for staff to flag any identified risk, so that once implemented all staff will have this link.	Cheryl Hughes- Dec 2019
3. We will be rolling out a corporate training programme and including risk as a topic available to all staff and compulsory for service managers and project leads	Cheryl Hughes/ Annette Cardy- Feb 2020
4. Elected members and senior staff will be approached as part of the development of the policy, and to factor in risk appetite	Cheryl Hughes- Nov 2019

Risk Maturity Assessment – Risk Assessment			
1.	**Risk Identification:**	**✓/✗**	**Evaluation**
1.1	Comprehensive process in place for systematically identifying risks throughout the organisation.	✓/✗	Risks are identified annually in the process of developing Service Plans. Any risks to the achievement of objectives for that Service are recorded as risks. Risks are then scored and, if they hit a certain threshold, will be required to be added to the Corporate Risk Register via TEN. Those below the threshold remain on the Service Plan only. Risks are then able to be identified and added throughout the year at forums such as CLT. However, risks appear to be mainly the consideration and responsibility of management. Further, complaints received by the Council are not analysed for trends and to identify potential risks. Further, there appears to be no ICT risks held on the CRR.
2.	**Risk Analysis:**		
2.1	Risks are linked to objectives	✗	Risks are not linked to the corporate objectives of the Council

2.2	Risks are clearly described	✗	The Risk Management Policy provides guidance on the best way to describe a risk with the consequence required to be included. However, this is rarely seen as part of risk descriptors and, therefore, they do not detail the actual risk.
2.3	Risks are assigned a category	✗	Risks are not assigned a category
3.	**Risk Evaluation:**		
3.1	Risks are evaluated based on a defined scoring methodology	✓/✗	All risks are assessed on a defined scoring methodology with a 4x4 risk matrix in place identifying the potential impact and likelihood. A risk assessment table is also found within the Risk Management Policy with the impact further defined for different scenarios. However, use of the 4x4 risk matrix results in risks either being serious enough to be added to the CRR or not serious enough to require mitigating actions (as per the Risk Management Policy), with no middle ground.
3.2	Regular management challenge of the risk evaluations applied	✓	Risk scorings on the CRR are discussed at CLT on a regular basis. In addition, an annual review of the CRR is completed, as per policy, to ensure that risk scoring is still appropriate. This was seen working well in relation to the housing land supply risk which has recently increased due to decisions made my Members.
5.	**Assigning responsibilities for risk:**		
5.1	All risks have an owner	✓/✗	There are 17 risks found on the CRR with all having an owner, albeit two are the responsibility of the CLT. Risks on the service plans are assumed to be the responsibility of the service manager but this is not explicitly stated.

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

Recommendations for improvement – Risk Assessment
1. Risk identification processes should be expanded within the Risk Management Policy to ensure staff at all levels are able to identify and escalate risks and these should be discussed in Service Level meetings on a monthly basis. Complaints should also be reviewed to identify any trends. 2. An updated scoring matrix (5x5) should be considered to provide a more differentiated score for the risks at all levels of the Council 3. All risks identified should be added to the Council's risk management software to allow for service level risk registers to be produced and maintained as well as having a centralised repository of risks to allow for greater visibility of risks across the Council 4. Risks should be assigned a category in order to undertake more informed trend analysis. This will become a more valuable tool when all risks are added to the Council's new risk management system 5. The approach to writing a risk should be updated in the Risk Management Policy with current risks reviewed to ensure they are appropriate. See Appendix III for an example of how to write risks as seen at another client

Management Response	Responsibility and Implementation Date
We will be reviewing and updating the risk management policy and will factor these recommendations into the review and roll out of this.	Cheryl Hughes, December 2019

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.
2.	**Action Plans:**		
2.1	Action plans are in place for all risks that have not been accepted at the current level.	✓/×	A sample of risks were viewed on TEN, all of which had mitigating actions. However, some actions were not considered sufficiently clear or specific such as 'Improve Project Management' whilst others had completion dates that had passed or were too far in the future, such as 2029. In addition, service level risks did not all have mitigating actions.

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

Recommendations for improvement – Risk Mitigation

1. All risks, including those on the Service Plans, should have associated actions with target dates and responsible officers

2. Actions that have completion dates that have passed should be reviewed to ensure they are still valid with dates updated where necessary. Actions due to be completed in 2029 are to be reassessed and identified if they are in fact controls and, therefore, do not require updates each quarter for the next ten years.

Management Response	Responsibility and Implementation Date
As part of a wider project to move from TEN software, we will be reviewing the current risks and mitigating actions and how they are reported. We are aware that in the current software we have 'expired' risks and that some housekeeping needs to be done as part of the wider software upgrade	Cheryl Hughes/ Eloise Howard- Jan 2020

Risk Maturity Assessment – Reporting and Review			
1.	**Monitoring:**	**✓/×**	**Evaluation**
1.1	A strategic risk register has been populated	✓	A Corporate Risk Register is in place and is reviewed on a quarterly basis
1.2	Departmental risk registers have been populated	✓/×	Formal service level risk registers are not in place within the Council. However, risks not scoring over a certain threshold are to be found on the Service Plans. These are updated throughout the year with risks able to be added if identified. However, as not held in a formal risk register, there is often a lack of information such as due dates, responsible officers, actions etc.
1.3	Risk registers are reviewed on a regular basis	✓	As discussed in 1.1 above, the CRR is reviewed quarterly and updated where required.
2.	**Reporting:**		
2.1	Regular reporting on key risks at corporate level	✓	The CRR is reported quarterly at the CLT after the updates have been received from the risk owners/action leads. Further, updates are taken to Audit Committee for awareness.
2.2	Regular reporting on risks at division/department level	✓/×	Through discussion with Managers, discussion of risks at service levels do appear to take place but to varying degrees, likely due to the lack of formalised guidance.
2.3	Decisions based on risk reports are fed back	✓/×	Due to a lack of discussion on operational risks, and therefore risks that are more relevant to the services, this feedback is limited. However, there are forums for this to take place.
3.	**Assurance:**		
3.1	Assurance is provided on the effectiveness of the management of risks	✓/×	Whilst there is good oversight of risks at a Corporate level, only a limited level of assurance is able to be provided that risks are effectively being managed at service level.

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

Recommendations for improvement - Reporting and Review
1. The Risk Management Policy should be updated to ensure that discussion of risks form a consistent part of service level meetings, perhaps through the use of a standardised agenda

Management Response	Responsibility and Implementation Date
A full review and update of our risk management policy will be taking place	Cheryl Hughes, December 2019

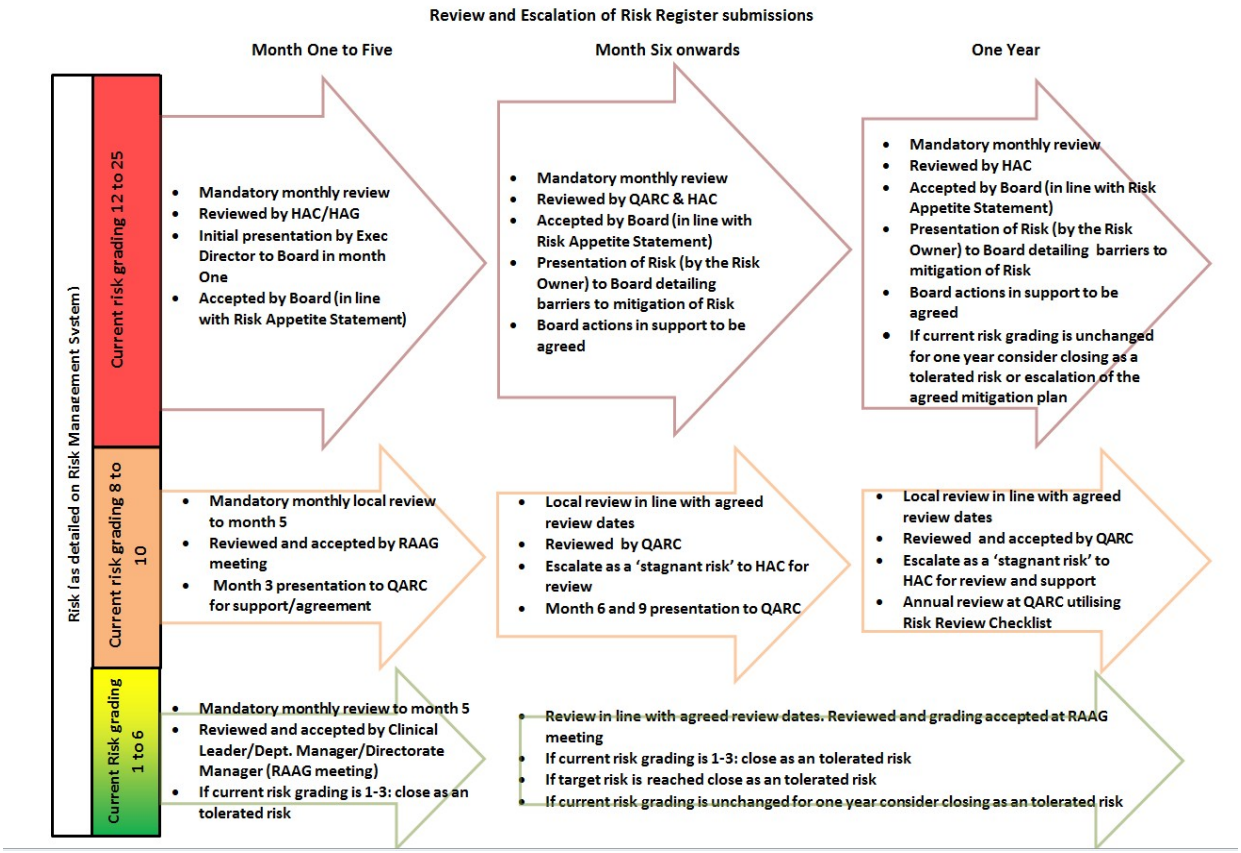
Risk Maturity Assessment – Continuous Improvement			
1.	**Continuous Improvement:**	**✓/×**	**Evaluation**
1.1	The organisation's risk management approach and the Board's risk appetite are regularly reviewed and refined in light of new risk information reported	✓/×	The Council reviews its Risk Management Policy every three years, with the next review set for 2020. However, due to the changes across the Council and the appointment of a new lead for risk, there are plans in place to review the policy before this date. Whilst there is no indication of regular reviews of the Council's formal approach to risk management occurring as the result of new risk information being reported, this may be due to a lack of significant risk requiring this to be done. Further, with the change in staff and structure across the Council, it is likely that changes will occur.
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 itself does not monitor and report on any KPIs relating to risk management.

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

Recommendations for improvement – Continuous Improvement	
1. Identify KPIs in order 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 I for a list of possible KPIs	
Management Response	Responsibility and Implementation Date
We are currently reviewing and overhauling all performance management, and as part of the balance scorecard dashboard, we will look to include KPI's around risk, as well as reporting risk updates.	Cheryl Hughes/ Eloise Howard- Feb 2020

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 Board/Committee meetings and departmental governance group meetings and ensure that a designated deputy attends in their absence



APPENDIX II - EXAMPLE RISK APPETITE STATEMENT

The Council recognises it is impossible to deliver its services and achieve positive outcomes for its stakeholders without taking risks. Indeed, only by taking risks can the Council realise its aims. However, it must take risks in a controlled manner, thus reducing its exposure to a level deemed acceptable from time to time by the Council and, by extension, external inspectors/regulators and relevant legislation.

Methods of controlling risks must be balanced in order to support innovation and the imaginative use of resources when it is to achieve substantial benefit. In addition, the Council may accept some high risks because of the cost of controlling them. As a general principle, the Council will not accept and will therefore seek to control all risks, which have the potential to:

- Cause significant harm to staff, visitors, contractors and other stakeholders;
- Endanger notably the reputation of the Council;
- Have severe financial consequences which could jeopardise the Council's viability;
- Jeopardise significantly the Council's ability to carry out its normal operational activities;
- Threaten the Council's compliance with law and regulation.

Risk Tolerance

The Council has determined that some risks are acceptable / tolerable. This is in line with the stated risk appetite and is reflected in the green area of the risk heat map. All risks with a rating of three or less are deemed to be acceptable or tolerable. Some risks with a rating higher than three may also be accepted/tolerated. This would most probably be because of the potential benefits of taking the risk, the cost of controlling the risk or the risk's proximity; acceptance or tolerance of any risk with a rating higher than 3 must be approved by a director or manager with the appropriate authority to do so (not the risk owner).

APPENDIX III – EXAMPLE RISK DEFINITION GUIDANCE

A risk is something that might happen that could have an effect upon the Council.

The risk will be a combination of three elements:
Cause – what might trigger the event to occur
Event – an unplanned or unintended variation from an objective
Effect – how the Council may be impacted should the event occur

Articulating the risk from these three elements will result in the risk starting with the word ***'If' (the cause)***, with a middle section ***'then' (the event)***, and a final section ***'resulting in' (the effect)*** or similar terminology.

Risk identification – getting it wrong! It is NOT something that has happened (an incident) or something that will happen or is already happening (an issue). The following descriptors should NOT be used:

Failure of or questioning the objective
One word risks
Statement of fact
Failure to ….
Whinge!
Essay

APPENDIX IV - 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.	There is some discussion around the review and update of the organisations approach to risk management based on information received/changes to the organisation whilst KPIs are not formally reviewed or reported at a corporate level.
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.	The Board gets minimal assurance 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 V - 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.

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

The key risks, and therefore the lines of enquiry which we will undertake as part of our review in order to assess if the controls relating to Risk Management are working effectively are::

- Whether there is a clear understanding of risk within the Council;
- The risks on the risk registers correspond to those actually facing the Council;
- Risks are reviewed on a regular basis and appropriate assurance and controls are assigned to them; and
- Escalation and management review of risks is sufficient, and mitigating actions are effective

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; and
- 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.

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

ADDED VALUE

The review will enable us to benchmark the Council's risk maturity level against other Councils.

BAF/CRR REFERENCE:

N/A – This audit will be reviewing the BAF and Risk Register as part of the scope.

DATA ANALYTICS

We can perform high level analytics on the meta data in the risk registers and present these in a graphical format.

EXCLUSIONS

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.

FOR MORE INFORMATION:

Greg Rubins

greg.rubins@bdo.co.uk

www.bdo.co.uk