BOROUGH COUNCIL KINGS LYNN AND WEST NORFOLK

To: **Management Team & Ged Greaves, Corporate Performance Manager**

Author: **Faye Haywood, Internal Audit Manager for Borough Council Kings Lynn and West Norfolk**

Subject: **Results from Internal Audit Assessment of Risk Management Maturity with suggested recommendations for improvement.**

Recommendations:

1) That senior management consider recommendations contained within this report to enhance the level of risk maturity and adopt an Enterprise Risk Management approach towards risk management.

1.0 BACKGROUND

1.1 The role of the Internal Audit Manager for the Borough Council of King's Lynn and West Norfolk is now being carried out by Eastern Internal Audit Services (EIAS). The arrangement started formally in June 2021. Faye Haywood from South Norfolk Council provides the in-house Internal Audit team with management support.

1.2 As part of this role, the Internal Audit Manager has carried out an assessment of the Internal Audit function against the Public Sector Internal Audit Standards (PSIAS) to highlight any areas where improvements may be required. This exercise was necessary for the Internal Audit Manager to determine how much reliance can be placed on the assurances coming from the function, which are used to determine the annual opinion on the Governance, Risk Management and Control at the Council.

1.3 As part of the above assessment and in conformance with the PSIAS 2010 planning standard, the report presented to the Audit Committee in October 2021 recommends that the Internal Audit Manager undertake a review of the Council's risk framework and maturity before developing a risk-based internal audit plan.

1.4 The assessment allows the Internal Audit Manager to evaluate the level of reliance that can be placed on the assessment of risk at the Council and where applicable, suggest recommendations if improvements are required. This exercise was undertaken ahead of the Internal Audit planning process for 2022/23 and informed the internal audit planning approach.

1.5 This report therefore contains the observations and recommendations from the assessment for management consideration with the aim of enhancing the approach to risk management and increasing the risk maturity of the council.

Introduction to Enterprise Risk Management (ERM)

1.6 The Internal Audit team advocates the adoption of Enterprise Risk Management (ERM) framework. ERM is now successfully used around the world, across industries and in organisations of all types and sizes to enhance resilience, adapt to change and ultimately increase the likelihood of aims and objectives being achieved. Enterprise risk management is a holistic way to effectively manage risk across an entire organisation. A well-managed

ERM framework can facilitate more effective risk discussions and risk taking within the boundaries of a pre-agreed appetite.

1.7 Traditional risk management often identifies and manages opportunities and risks in isolation. An ERM approach advocates the use of training, sets clear boundaries, and facilitates good communication to allow the organisation to be better prepared, adapt and spot the interdependencies of risks that threaten growth, performance and success. Some of the benefits that can be realised form the ERM approach include:

- Greater focus on the threats to strategic delivery that really matter;
- Risk focused culture; facilitates discussion about risk at all levels;
- Improved perspective; a complete viewpoint on risk that supports early detection, and an opportunity to exploit opportunities;
- Efficient use of resources; consistent analysis of risks allows the Council to prioritise the most appropriate response.

2.0 METHODOLOGY

2.1 The risk maturity assessment from The Chartered Institute of Internal Auditors has been used to compare the risk management framework at the council against five stages of risk maturity.

2.2 A set of characteristics has been defined for each of the maturity levels. The maturity levels are as follows:

Risk Naïve	No formal approach developed for risk management
Risk Aware	Scattered silo-based approach to risk management
Risk Defined	Strategy and policies in place and communicated. Risk appetite defined.
Risk Managed	Enterprise approach to risk management developed and communicated
Risk Enabled	Risk management and internal controls fully embedded into the operations.

2.3 Evidence was requested and collected by the Internal Audit team and discussions held with the Corporate Performance Manager to ascertain which level of maturity applies in 13 areas.

2.4 The outcomes of this assessment can be used to guide policy improvements and aid Internal Audit's approach to planning. This exercise also highlights any areas where the Internal Audit team can facilitate and support the improvement of risk management.

3.0 OUTCOMES

3.1 **Appendix one** provides further details regarding the results of the assessment in full.

3.2 Areas of the risk maturity assessment scored positively at Borough Council of Kings Lynn and West Norfolk. In seven areas the Risk Defined category was observed. The Council has defined its strategic objectives and each risk has been raised in relation to achieving the corporate objectives. The Risk Management Strategy document has recently been reviewed and explains the roles and responsibilities of staff in managing strategic and operational risk. A risk scoring system has been defined and evidence was provided showing the strategic risks of the council being reviewed by Management Team and the Audit Committee. A commitment has also been made to reviewing risks more regularly in accordance with the updated strategy.

3.3 A risk defined maturity can be observed overall, however, there are areas which require improvement to bring the Risk Management approach in line with best practice and increase risk maturity. A total of six areas are currently consistent with the lower end of the risk maturity scale. The lowest maturity 'Risk Naïve' can be observed in two areas. The following section provides details of the observations and improvement recommendations to enhance the Councils risk maturity in these areas.

3.4 **The risk appetite of the organisation has not been defined in terms of its scoring system.**

Within the risk strategy document, likelihood and impact descriptions have been defined in terms of scoring for a range of different categories such as impact on service and personal safety etc. The combined likelihood and impact score from low to high has been defined, colour coded and descriptions of how each level of risk should be managed has is outlined. The risk appetite statement is not however defined in accordance with the scoring system.

The Risk Management Strategy describes the council's risk appetite in the following way;

This is 'the amount of risk that an organisation is willing to seek or accept in the pursuit of its long-term objectives'. The council's risk appetite is defined in the Risk Management Policy as 'open', which means that the council is 'prepared to consider all delivery options and select those with the highest probability of productive outcomes, even when there are elevated levels of associated risk'.

Practically, it is difficult for risk owners to apply the council's 'open' policy when deciding upon the level of mitigating action that should be applied to ensure risk taking is within acceptable boundaries.

Additionally no assurance can be provided that risks have been managed and mitigated to an acceptable level if the acceptable level cannot be tangibly demonstrated.

Furthermore the Risk Management Strategy advises that *'Where officers have concerns about risks, they should be reported to the relevant director or Policy, Performance and Personnel. These concerns may for example include Operational risks that have identified a potential strategic risk and risks that move outside the appetite boundaries'.*

The above does not clearly outline at what score a risk should be escalated. Whereas, defining the councils risk appetite in terms of the scoring system will allow officers to easily identify risks that are determined to be outside of the appetite boundaries. i.e. any risks that are high scoring are outside the council's risk appetite and need to be appropriately escalated. Similarly, any risks that are mitigated to a medium or low score could be de-escalated to an operational risk register for monitoring.

Defining the appetite in terms of scoring system allows the council to effectively use resources to target the most significant scoring risks and demonstrate it is managing risk in line with a defined appetite level.

3.5 **Management have not been recently trained to understand what risk is, and their responsibility for managing risk.**

The Risk Management Strategy states the following: '*Risk management training will be provided to relevant officers with the aim of ensuring that they have the skills necessary to identify, appraise and control the risks associated with the services they provide and*

projects that they manage. Elected members will receive training on risk so that they can consider the implications of risk whilst engaged with council activities'.
We were unable to obtain evidence to show that management or members had been recently trained in risk management.

The Policy and Performance Team have already identified the need for a training programme to be developed and have approached Internal Audit for support for training for officers and relevant members.

3.6 **Responses to the risk have not been selected and implemented**

The Risk Management Strategy outlines four responses to risk, which are; Avoidance, Transfer, Mitigate, and Acceptance. The council's corporate risk register does not however provide details of the response to each of the risk identified. This is relative to the earlier point made regarding defining the appetite in terms of scoring in that, the response to the risk can be informed by whether the score is outside of the council's appetite to ensure effective use of resources.

3.7 **All risks have not been collected into one list. Risk has not been allocated to specific job titles at Directorate level.**

The corporate and strategic risks are collated into one list and senior responsible officers have been assigned to each risk, mitigating actions are provided and progress against these reported.

The council's risk management strategy has been recently updated to allow for directorate risk registers to be held by each service area with the aim of making the corporate risk register more manageable. The council has also committed to ensuring that all major project registers are completed.

At the time of undertaking this assessment, just one directorate register was provided for Resources and one project register for West Winch. It was noted that the template for the directorate risk register does not currently allow for a responsible officer to be added to each risk.

It is understood that the work to rationalise the strategic register and produce directorate and project risk registers is ongoing however it is recommended that all strategic, directorate and project risk registers follow the same layout. This is to ensure that all risks are comparable at all levels and that they can be escalated and de-escalated without additional information having to be provided.

3.8 **Risks are reported where responses have not managed the risks to an acceptable level**

As observed within point 3.4 regarding risk appetite, it is not possible to ascertain whether risks are managed to an acceptable level as this has not been defined in terms of the scoring system. In addition to this, it is not clear from the current corporate risk monitoring report template whether the completion of risk mitigating actions are lowering each risk score.

It is therefore recommended that once the register has been rationalised and risk response section added and appetite defined in terms of the scoring system, that the register layout is updated to incorporate original and target scores for each risk.

The risk reporting layout should allow for an assessment to me made on whether risks are being managed to an acceptable level. This assessment allows senior management to manage progress more effectively and Audit Committee to fulfil its terms of reference when evaluating whether the Council is managing risk in accordance with its strategy.

3.9 **Managers do not provide assurance on the effectiveness of their risk management**

There is currently no mechanism for management to provide assurance that they have effectively managed risks relative to delivery of their service objectives. Typically this is achieved by other local authorities by obtaining a self-validated statement from Assistant Directors which feeds into the council's annual governance statement.

4.0 RECOMMENDATIONS

4.1 The Council to consider defining its risk appetite by aligning it to the existing 5X5 scoring system and impact likelihood descriptions. This will allow for a mechanism for risk escalation and de-escalation and the risk response and actions to be designed and prioritised based on the perceived severity of the risk. This approach will also highlight where risks are not being managed in line with appetite expectations and give an indication for risk taking capacity. It will also allow any high scoring risks regardless of where they originate to be escalated to the strategic register for oversight and management action to prioritise mitigation efforts.

4.2 A risk management training programme to be developed for managers and members where relevant to complement and promote the revised risk management strategy document with the aim of enhancing the risk management culture.

4.3 The corporate risk register template to be updated with a risk response column. Allowing officers to select one of the four responses highlighted in the Risk Management Strategy, which are Avoidance, Transfer, Mitigate, and Acceptance.

4.4 All strategic, directorate and project risks are identified and assessed using the same register template. This is to ensure that all risks are comparable at all levels and that they can be escalated and de-escalated without additional information having to be provided.

4.5 The corporate risk monitoring report is updated to provide assurance that risks are reducing through the completion of mitigating actions.

4.6 A methodology be designed to allow management to provide assurance that their service risks are being effectively managed.

4.7 Once agreed and implemented the above recommendations to be reflected in an updated version of the Risk Management strategy/policy.

5.0 CONCLUSION

Overall the councils risk management approach is currently consistent with a 'Risk Defined' maturity, however characteristics within the risk naïve and risk aware were also observed. We, therefore, recommend improvements are made to the existing framework support an enhanced approach to risk management assurance. Once implemented these improvements will allow the Council to benefit from the advantages of an Enterprise Risk Management Framework.

Background papers: - None

Lead Contact Officer
Name and Post: Faye Haywood Internal Audit Manager for Borough Council Kings Lynn and West Norfolk
Telephone Number: 01508 533873
Email: fayehaywood@southnorfolkandbroadland.gov.uk;

Appendices attached to this report: Risk Maturity Assessment BCKLWN 2022

Appendix 1 – Risk Maturity Assessment BCKLWN 2022

Key Characteristics	Risk Naïve	Risk Aware	Risk Defined	Risk Managed	Risk enabled	Evidence
Process	No formal approach developed for risk management	Scattered silo-based approach to risk management	Strategy and policies in place and communicated. Risk appetite defined.	Enterprise approach to risk management developed and communicated	Risk management and internal controls fully embedded into the operations.	
1. The organisations objectives are defined	Possibly	Yes but may be no consistent approach	Yes	Yes	Yes	Corporate plan includes five key themes with a number of objectives directly attributing to the corporate themes. Themes are: Focusing on delivery Delivering growth in the economy and with local housing Protecting and enhancing the environment including tackling climate change. Creating and maintaining good quality places that make a positive difference to people's lives. Helping to improve the health and wellbeing of our communities. The corporate risk register ties each risk back to each corporate theme.
2. Management have been trained to understand what risk are, and their responsibility for them	No	Some limited training	Yes	Yes	Yes	Policy and guidance provide guidance however no formal/informal training offered to staff or members recently. The RM Policy includes the following on training; *Risk management training will be provided to relevant officers with the aim of* *ensuring that they have the skills necessary to identify, appraise and control* *the risks associated with the services they provide and projects that they* *manage. Elected members will receive training on risk so that they can* *consider the implications of risk whilst engaged with council activities.*
3. A scoring system for assessing risk has been defined	No	Unlikely, with no consistent approach defined	Yes	Yes	Yes	Yes a 5X5 matrix has been defined in the Council's Risk Management Strategy with definitions for impact and likelihood scales in categories of risk.

Key Characteristics	Risk Naïve	Risk Aware	Risk Defined	Risk Managed	Risk enabled	Evidence
4. The risk appetite of the organisation has been defined in terms of the scoring system	No	No	Yes	Yes	Yes	No the risk appetite of the Council is determined in terms of a statement - Open 'prepared to consider all delivery options and select those with the highest probability of productive outcomes, even when there are elevated levels of associated risk'. Practically this would be difficult to interpret when scoring each risk. The strategic risk register is not clear about which risks are currently over the risk appetite of the Council.
5. Processes have been defined to determine risks and these have been followed	No	Unlikely	Yes, but may not apply to the whole organisation	Yes	Yes	Processes have been defined with the Councils risk management Strategy. De-escalation and escalation protocols are reliant upon staff informing the Policy and Performance Team. Defining the risk appetite with the scoring system would be a way to ensure that any high scoring risks were appropriately escalated. The Strategic/corporate risk register follow processes outlined in the RM Strategy. One example obtained showing Directorate level risk management. Unconfirmed whether the rest of the service areas yet follow this process. Strategic/Corporate template is not followed in directorate registers.
6. All risks have been collected into one list. Risk has been allocated to specific job titles	No	Some incomplete lists may exist	Yes, but may not apply to the whole organisation	Yes	Yes	Strategic risks are in one list. Directorate and project risks will be held separately. The strategic risk register does not allocate specific job titles currently. The new strategy indicates that Directors will be assigned to each risk. The Resources Directorate register does not assign accountability to individuals.
7. All risks have been assessed in accordance with the defined scoring system	No	Some incomplete lists may exist	Yes, but may not apply to the whole organisation	Yes	Yes	Yes a 5X5 matrix has been defined in the Council's Risk Management Strategy with definitions for impact and likelihood scales.
8. Responses to the risk have been selected and implemented	No	Some responses identified	Yes, but may not apply to the whole organisation	Yes	Yes	Risk responses are defined within the strategy but are not outlined in the register.

Key Characteristics	Risk Naïve	Risk Aware	Risk Defined	Risk Managed	Risk enabled	Evidence
9. Management have set up methods to monitor the proper operation of key processes, responses and action plans	No	Some monitoring controls	Yes, but may not apply to the whole organisation	Yes	Yes	The Risk Management Strategy outlines how risks will be monitored by Management Team, Service areas and the Audit Committee in line with its TOR. The Strategy outlines the circumstances whereby risks should be escalated to senior management but this is reliant on responsible officers following the strategy. Evidence of risks being removed from the register is however available and risk scores increasing following review. To strengthen the process, risks could escalate/de-escalate based on score. Unclear what the process is for monitoring risk at directorate level and lower. Strategy defines expectations but paper to Audit Committee identifies that all operational risks are due to be identified in service plans suggesting that this work is ongoing.
10. Risks are regularly reviewed by the organisation	No	Some risks are reviewed, but infrequently	Regular reviews probably annually	Regular reviews probably quarterly	Regular reviews, probably quarterly	Yes in line with Risk Management Strategy strategic/corporate risks are to be reviewed six monthly, however latest paper to Audit Committee suggests three times a year. The Strategic Risk Register contains 40 risks currently.
11. Management report risks to directors where responses have not managed the risks to a level acceptable to the board	No	No	Yes, but may be no formal process	Yes	Yes	No the risk appetite of the Council is determined in terms of a statement - Open 'prepared to consider all delivery options and select those with the highest probability of productive outcomes, even when there are elevated levels of associated risk'. Practically it would be difficult to identify risks that fall outside of the appetite of the Council and this information is not recorded against each risk. The corporate risk reporting template isn't clear in terms of the original score current score and target score making it difficult to gain assurance that risks are being mitigated.

Key Characteristics	Risk Naïve	Risk Aware	Risk Defined	Risk Managed	Risk enabled	Evidence
12. All significant new projects are routinely assessed for risk	No	No	Most projects	All projects	All projects	Project risk registers are not currently managed for all projects. As per latest Audit Committee paper: The current risk management strategy refers to roles and responsibilities. Project managers are identified and references are made to project risk registers. These registers are not collated corporately and the onus is on project managers to notify relevant Executive Directors of significant risks and review risks. 3.7.2 Property Services and Major Housing Projects will have in place a risk register for each approved capital project. 3.7.3 A risk register has been developed for the West Winch Growth Area and this is reported to the West Winch Project Board and Officer Major Project Board. 3.7.4 Governance processes related to the Towns Fund are developing and risk is incorporated into documents presented to the Town Deal Board and Programme Board. 3.7.5 The Member Major Project Board role includes the oversight and monitoring of the delivery of the programme of Major Projects. The Board will make recommendations to Cabinet and could inform Policy Review and Development Panels and other committees. Its oversight will cover several of the project risks included on the corporate risk register for example West Winch, the Accelerated Construction Programme, Major Housing Projects, regeneration projects such as the South Gate area and the Town Deal. As part of the rationalisation of the corporate risk register these projects could be replaced by a high-level programme risk on the corporate risk register. It is unclear whether the project registers follow the corporate template.

Key Characteristics	Risk Naïve	Risk Aware	Risk Defined	Risk Managed	Risk enabled	Evidence
13. Responsibility for the determination assessment and management of risk is included in job descriptions	No	No	Limited	Most job descriptions	Yes	Not tested.
14. Managers provide assurance on the effectiveness of their risk management	No	No	No	Some managers	Yes	There is no formal approach to obtaining assurances on the effectiveness of risk management.
15. Managers are assessed on their risk management performance	No	No	No	Some managers	Yes	Not tested.
Total:	2	4	7	0	0	