SUBJECT:	**RISK MANAGEMENT**
REPORT OF:	**Director of Resources**
REPORT AUTHOR	**Director of Resources**
WARD/S AFFECTED	**N/a**

1. Purpose of Report

1.1 The purpose of this report is to update Members on risk management across the two authorities.

RECOMMENDATION

The Committee is asked to note the report

2. Information

2.1 The report will inform members about:

- Work to maintain awareness of the importance of risk management.
- The processes for reviewing main operational risks and financial risks
- Information Governance risks
- The strategic risks

2.2 During the last year work has been undertaken to maintain awareness of risk management and how it is integral to the way the organisation needs to work. This has been by communications through staff newsletters, posters and material to be used at team meetings.

2.3 Currently work is in hand to develop a training session that will be part of the Middle Managers Development Programme, which will focus on managing risks during periods of change and transformation. The intention is to help managers identify and mitigate these risks and to stimulate debate between themselves on the key issues.

2.4 The Internal Audit work programme continues to be shaped by reviewing the risk profile of the authorities. This has ensured audit work has looked at issues such as the effectiveness of controls following changes to new shared service teams and the project to create a unified ICT infrastructure.

2.5 The key operational risks are reviewed monthly by the Management Team and Heads of Service. Over the course of the year the most high profile risks which has required action have been:

- Levels of temporary accommodation
- Work pressures on the Planning Service and staffing issues
- Work pressures on the Property team.
- The performance of the Councils' telecommunications contractor.

2.6 Financial risks are reviewed each year as part of the budget process and are clearly set out in the documentation related to the setting of the Councils' budgets. The risks are also identified within the Medium Term Financial Strategies. The main financial risks are currently assessed as:

- Responding to the significant reduction in Government funding, and the Council's ability to adjust its net expenditure base to cope with the reductions.

- The cost of major planning inquiries, enforcement actions or responding to national infrastructure proposals that impact on the area.

- The costs of temporary accommodation, and supporting solutions to the temporary accommodation issue.

- Shortfall on income targets.

2.7 During the past year the Councils have continued to improve their control and processes of Information Governance. This has included developing an Information Governance risk register (Appendix A). The most significant risk and is one that is the focus of work in the coming year, is poor file management causing inefficient working, unnecessary storage costs, data loss and poor decision making. Work is in progress to improve file management of physical records and services have made significant progress in disposing of material not required or out of date, and improving the organisation and recording of retained material.

2.8 The larger challenge lies with improving the management of electronic information, and this includes information held in personal email storage. Work is in hand to change working practises going forward, and to tackle the volume of historic emails.

2.9 The Strategic Risks for the Councils are reviewed quarterly by senior management and the main strategic non- financial risks are currently assessed as:

<u>Affordable Housing</u>
Increase in temporary accommodation numbers, migration of young people and families out of area affecting sustainability of communities.

<u>Major Infrastructure Projects Impacts.</u>
Detrimental impact on local communities and environment. Costs to authorities in defending local area from worst impacts

2.10 These risks are at the centre of a number of pieces of work being undertaken by the Councils and other bodies.

2.11 Over the last year the level of insurance claims in both authorities has remained low, less than ten claims per annum. There have been no significant H&S issues, or breeches of data security.

3. Consultation

Not applicable

4. Options

Not applicable

5. Corporate Implications

4.1 Comment from the Internal Auditor: Risk management is an important part of the governance and control framework for the two Councils and is subject to a biannual internal audit. Internal Audit are pleased to note, from their earlier work, that the two Councils have embraced good risk management processes which are now becoming embedded within the day to day management and delivery of the Council's services. Despite the significant transformational changes that have occurred over the last couple of years risk management has remained high on the agenda for the Council's officers and the control framework has remained sound during this period of change. Internal audit work will continue to test the resilience of risk management in future years.

4.2 There are no financial implications arising from this report, nor any any implications for the Council's policies and procedures.

6. Links to Council Policy Objectives

6.1 Risk management is one of the main elements of corporate governance. Effective organisations have a proactive approach to risk management.

7. Next Steps

7.1 Not applicable.

Background Papers:	None

APPENDIX A

INFORMATION RISKS

Risk Description	Trigger	Control	L	I	Score	Officer
Poor file management causing inefficient working, unnecessary storage costs, data loss and poor decision making.	• Information held in personal files or email folders, not accessible or known about by other staff and managers. • Data held in unstructured files making search/retrieval difficult • Difficulty in retrieving and matching information • Inhibitor to service change • Information held past its disposal date, may be out of date and inaccurate • Business continuity issues	• Understanding embedded in teams about the importance of IG. • Guidance and training provided on file management. • Avoid service information being stored in personal files, control use of C/ drives • Retention policies in place and adhered to. Clear guidelines on how to judge retention requirements. • Accountability for data sets clear, Information Asset Register in place and maintained. • Efforts made to reduce and ultimately eliminate email storage of data. • Address issue of Planning W drive for SBDC. • Controls in place for onsite file storage, identifying process to log location of files, data owners and destruction dates.	4	3	12	IAO (HoS)

Risk Description	Trigger	Control	L	I	Score	Officer
Uncontrolled data sharing leading to ICO audit, legal challenges.	• Challenge reveals absence of clear documented basis for data sharing. • Sharing of data not supported by resident/client agreements • Absence of privacy impact assessments. • Legal action against the Council • Failure to meet requirements of DPA (GDPR)	• Data sharing protocols in place • Staff understand the risks associated with data sharing, and then manage the risks. • Privacy Impact assessments undertaken. • Where data is collected and will be shared, clear resident/client agreement to sharing exists (wording on forms etc). • Compliance with guidance andrequirements of ICO (e.g. GDPR)	3	3	9	IAO (HoS)
Data unreliable or inaccurate, leading to reputation damage, residents not using Council information sources.	• Poor decision making • Poor customer service due to incorrect information being provided.	• Clear ownership for datasets responsibilities in job descriptions • Retention and disposal policies • Data quality standards in place and monitored.	2	3	6	IAO (HoS)
Loss of information due to poor security and control.	• Physical loss of information, whether electronic or physical. • Corruption of information • Damage to information caused by third party actions	• Training of staff on data protection, password security etc. • Security controls in place (e.g. passwords; encryption) for fixed and portable devices.	2	3	6	IAO (HoS)

Risk Description	Trigger	Control	L	I	Score	Officer
		• Measures in place to minimise risk of cyber attack. • Obligations on contractors clear • Business continuity arrangements in place • Information stored in safe and secure manner, ideally electronically.				
Poor management of FoI requests.	• Failure of system used for FoI • FoI system ceases to be fit for purpose • Staff do not understand properly FoI system and processes. •	• Ensure FoI system remains fit for purpose, re-procure if necessary. • Test resilience of FoI system • Ensure staff training on systems and processes up to date especially for new starters.	2	3	6	HoBS CIO