Corporate Risk Management: Developmental Objectives 2023/24

Ref:	Objective	Progress to date
1	To continue raising awareness and develop understanding of Risk Management across the organisation, by way of information sharing through the Corporate Risk and Resilience Group and targeted 1:1 training, as required.	The use of Microsoft Teams and SharePoint sites has enabled more regular risk communication and information sharing across the organisation. Enquiries and referrals have continued to increase in relation to risk management assurance, with all handled successfully to date. An examination of the nature of the enquiries was undertaken which indicated that the increase was due to greater awareness internally and because of increased scrutiny of risk management practices by stakeholders such as regulators and partners (such as those buying services from the Council). Another contributing factor has been the recruitment and changing roles of employees. Additional risk information and guidance has been provided at meetings of the Corporate Risk and Resilience Group and to Group Management Teams. The Corporate Risk Officer has assisted employees from across the organisation and has provided training throughout the year to both existing and new employees.

Ref:	Objective	Progress to date
2	To regularly review, update and enhance Business Impact Assessments and supporting service Business Continuity Plans, where assessed as necessary.	As part of the annual corporate exercise, Service Directors reviewed Business Impact Assessments and authorised subsequent Business Continuity Plans. This process was conducted in May 2023, November 2023 and again during April/May 2024, to ensure plans and mitigations were in place and regularly reviewed.
3	To ensure risk management activity is contributing to the achievement of Council priorities, outcomes, and delivery by reviewing the operational and strategic risk assessments and recording updates and revisions.	Work on this objective has focussed on the Corporate Risk Management Policy, which has been reviewed against the ALARM Risk Management Standard 2022 and the UK Government Orange Book (applicable to all government departments and parts of the UK public sector, with responsibility for public funds). The review confirmed that the Council's Risk Management Policy was still broadly fit for purpose, but highlighted areas that could be amended to reflect the latest industry standards. These areas have been updated and the revised Corporate Risk Management Policy was considered by the Cabinet in May 2024 where it was recommended for approval by Council, this is scheduled for July 2024. Reminders have been issued to all risk owners to review and update risk and control information. 1:1 assistance and support has been provided where necessary. Quarterly risk management updates have been provided to Group Management Teams and the Corporate Risk and Resilience Group for monitoring purposes.

Ref:	Objective	Progress to date
4	To develop risk management and business continuity performance including working in partnership with local resilience forums.	Officers from Risk Management and IT Services have attended several multi-agency events to share learning and share best practice from across partner organisations. This included participation in the 'Enabling Safe Business' series of events looking at the relationship between information risk, security and the wider operational risks associated with the region's public service organisations. Key risk management themes that were explored as part of the series included: Cyber resilience and business continuity, Public Services Network (PSN) compliance, Changes in data protection legislation, Cloud security and the wider cyber risk management landscape.
5	To prioritise critical IT systems and the links to critical service functions identified through the Corporate Risk and Resilience Group and the Business Continuity process.	To strengthen mitigation of cyber risks, the Council's Cyber Security Group (which includes representatives from Internal Audit and Risk Management) developed a new IT Security Policy and associated policies. The Council formally approved the new Information Security Framework and associated IT security sub policies. The sub policies relate to specific activities or functions within the council which expose the Council to risk. The Cyber Security Group has held meetings throughout the year to ensure the resilience of critical IT systems in response to increasing cyber threats. An internal audit was undertaken of the Council's IT Resilience and Disaster Recovery arrangements and an action plan has been agreed.

Ref:	Objective	Progress to date
		Workshops were conducted with the Leadership Team and the Risk and Resilience Group (exercise in a box) to raise awareness of the reliance on IT Applications for all business functions and the impact of an interruption to these, and to encourage participants to start thinking about the factors that would need to be considered in Continuity Plans to minimise the impact on service provision. The Business Impact Assessment framework and flow chart is currently under review to ensure Services adopt a consistent approach to considering the key factors in relation to an IT interruption and the development of effective continuity plans.