Corporate Risk Management: Developmental Objectives 2022/23

Ref:	Objective	Progress to date
1	Continue to develop understanding and awareness of Risk Management by way of best practice through the Risk & Resilience Group and directed training on request.	The deployment of Microsoft Teams and the use of SharePoint sites has enabled more regular risk communication and information sharing across the organisation. Additional risk information and guidance has been provided at meetings of the Corporate Risk and Resilience Group and to Group Management Teams. The contact details for service risk coordinators and staff within the Audit and Risk Service that are available on the Intranet page have been kept up to date throughout the year. 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	Business Continuity Plans will continue to be updated, enhanced and, where appropriate, formal testing against incident scenarios and best practice requirements will be carried out.	As part of the annual corporate exercise, Service Directors reviewed Business Impact Assessments and authorised subsequent Business Impact Plans. This was completed in May 2022, November 2022 and again during April / May 2023, to ensure plans and mitigation were in place and regularly reviewed in response to anticipated service delivery pressures.
3	The Operational and Strategic Risk Registers will be subject to periodic review for updates and revisions to ensure the continue to reflect and contribute to the achievement of Council priorities, linking risk management activity to outcomes and delivery.	Risk owners have been reminded and coached in how to keep risk information up to date and relevant. Regular risk management updates have been provided to Group Management Teams and the Corporate Risk and Resilience Group.
4	Continue to develop risk management and business continuity performance including comparison with other public sector organisations and local resilience forums.	Officers from Risk Management, IT Services and Emergency & Resilience Planning teams, have attended several multi-agency regional Local Resilience Forum events to share learning and share best practice from across partner organisations. This included participation in an immersive simulation of a ransomware attack organised by the Northern WARP (North East, Yorkshire & Humber and North West). The Northern WARP brings together three regional

Ref:	Objective	Progress to date
		Warning and Reporting Points that provide trusted safe spaces for alert, warnings, knowledge and experience sharing amongst public sector information governance and information security colleagues.
5	Continue to prioritise Critical IT systems and the links to Critical service functions identified through the revised Business Continuity process.	The Cyber Security Group has held meetings throughout the year to ensure the resilience of critical IT systems in response to increasing cyber threats. Several policies have been drafted during the year to enhance the Council's cyber security and its management of cyber risk. An internal audit was undertaken of the Council's IT continuity and recovery arrangements and an action plan has been agreed.