Report to: Audit & Accounts Committee Meeting 15 October 2025

Director Lead: Sanjiv Kohli, Deputy Chief Executive/Director of Resources (S151 Officer)

Lead Officer: Dave Richardson, Business Manager – ICT & Digital Services Ext 5405

Report Summary	
Report Title	Update on the LGA Newark and Sherwood District Council Cyber 360 Report
Purpose of Report	To present the updated results of LGA Newark and Sherwood District Council Cyber 360 Report
Recommendations	Members review, comment upon and note the update on the LGA Newark and Sherwood District Council Cyber 360 Report
Reasons for Recommendation	To provide Members with details and assurance from the LGA Newark and Sherwood District Council Cyber 360 Report

1.0 Background

1.1 The Local Government Association piloted Cyber 360 (C360s) peer reviews with several Local Authorities to ensure Cyber and information Security governance and culture is being understood and adequately resourced. The Cyber 360 Action Plan is not in the public area of the open report for security reasons and are held in the exempt version.

1.2 At the September 2023 Audit & Governance Committee the ICT & Digital Services Business Manager provided an update on the Cyber360 action plan and assurance that we are addressing any areas of cyber risk.

1.3 A Cyber360 action plan has been commissioned off the back of the report and regularly updated by the Corporate Information Governance Group (CIGG). Therefore, the updates to this committee will be provided by exception, on request or at least on an annual basis.

2.0 Proposal/Options Considered

2.1 The CIGG will continue the review of the Cyber360 action plan and provide updates. As of October 2025, 88% of the action plan is complete, with only 3 out of 24 tasks remaining.

2.2 It is important to note that further controls and measures have been implemented to enhance the Council's cyber resilience in alignment and exceeding the cyber security strategy 2022-2026.

2.3 The committee should note that a new digital strategy has been created and was approved by cabinet 9th September 2025, which embeds cyber security as a fundamental enabler of transformation. It focuses on strengthening digital trust through compliance with recognised standards (Cyber Essentials, ISO27001), adopting secure-by-design principles, and enhancing governance for data protection. Key actions include proactive risk management, continuous monitoring, and improved supply chain security. The strategy also prioritises staff awareness through training and cyber simulations, ensuring resilience against evolving threats while supporting innovation and safe delivery of digital services.

2.4 The landscape of cyber attacks is continuously changing, with threats becoming more advanced and varied. Recent incidents include attacks on JLR, airports and nurseries, as well as an incident affecting our supply chain. In recognition of this ever-changing environment, we have prioritised all key areas of cyber defence, including preparation, detection, response, containment and recovery. Particular emphasis has been placed on rigorous testing of our response and recovery processes to ensure resilience and readiness in the face of emerging cyber threats.

3.0 Implications

None.

Background Papers and Published Documents

Except for previously published documents, which will be available elsewhere, the documents listed here will be available for inspection in accordance with Section 100D of the Local Government Act 1972. Any documents that contain confidential information or personal information about individuals should not be included in this list.