Appendix B

OUTLINE SCOPE OF SOME AUDITS WITHIN AUDIT PLAN 2017/18

AUDIT AREA	OUTLINE SCOPE
Commissioning and Procurement	A review of the processes used in the Council for the commissioning and procurement of goods and services.
Effective Decision Making	Review of the process by which decisions (of all levels) are made in the Council, through the examination of alternatives, selection of choices and management of these choices to achieve business objectives.
Governance	A review of areas of governance including: - Governance and strategic direction (for example, are operational plans in place and communicated to officers?); - Accountability (for example, is there a clear organisational structure and are accountabilities delegated and understood?); - Ethics and Values (do senior managers promote ethics and values?); and - Results and performance (are plans linked to the Council's objectives, have appropriate performance measures been linked to planned outcomes and do senior managers monitor performance against plans?).
Payroll	Review the key controls related to HR and payroll within the Council, including use and development of the DigiGOV system.
Income (Education and Lifelong Learning)	Review the key controls related to income collection in schools, including development of charging and remissions policies, segregation of duties and VAT accounting.
Cradle to Grave contract audit	This is a review of a contract let by the Council from consideration of the outline business case to end of the contract, to include performance management. The review will focus on the key controls for all risks.
Cybersecurity Governance	This will require an evaluation of the governance, risk management and control processes in place and will include: - Cybersecurity response plan - Cybersecurity risks and threats - Cybersecurity Risk Register - Officer roles, responsibilities and training.
Inventory of information assets	Review the inventory of all information assets, including the existence and adequacy of preventative and detective controls and monitoring arrangements. Information assets include: - Data - Infrastructure - Applications - External relationships
Standard Security Configuration	Review security configuration management to establish if an accurate assessment of environments, based on risk, is achieved. Also, the processes in place to apply patches and updates.
Information Access Management	A review of account management, to include processes and procedures to grant, amend and remove access to systems, to include validating preventative control activities.
Response and Remediation	Review incident management and cybersecurity reporting arrangements. Assess vulnerabilities, analyse threat intelligence, and identify gaps.
On-going Monitoring	Review monitoring strategy, including: - Access level evaluation - Vulnerability assessment - Penetration testing - Malware - Incident response