1. Audit Summary – Core Systems Access Controls

Background and Context

1.1 The Council has many core IT systems, essential to running the Council, which are used to store, maintain, and access information. The management of user access is a critical control to ensuring that information is available and shared with only with those that require it.

1.2 A Logical Access Controls Policy is in place which sets out the requirements to ensure appropriate access control rules are in place across the Council's network and associated systems.

1.3 The Internal Audit of Cyber Security in April 2021 identified that regular reviews of user access were not taking place.

Scope and Objectives

1.4 The objective of this assignment was to review and assess the effectiveness of core system access controls. The audit aimed to provide an independent opinion on how effectively the risks associated with core system access were managed and provide assurance in respect of the following areas of risk:

- Policy was inappropriate and not understood by the business.
- User account provisioning was unauthorised.
- Leaver account access is not promptly revoked.
- Access rights were inappropriate for users.
- Monitoring of user accounts was ineffective.

Audit Opinion

1.5 Overall, Internal Audit obtained **"limited assurance"** on the adequacy and effectiveness of the Councils' Core Systems Access Controls arrangements. The risk is unauthorised access to sensitive data.

Key Messages and Findings:

1.6 The Logical Access Control Policy was appropriate, but there were significant control issues in the policy implementation and supporting processes. At the initial user provisioning stage for 'starters', controls were good.

1.7 Internal Audit raised two high priority and two medium priority findings. It was identified that ongoing monitoring, and prompt revocation controls were poor; there was no clear process to deal with 'movers'. For 'leavers' the HR and ICT processes were not adequately joined up and the current ICT infrastructure did not facilitate effective implementation of the Logical Access Control Policy. Internal Audit testing identified:

- That 16 of 155 'leavers' sampled had systems access recorded after their official leave date.
- Three out of four users of one core system had the ability to access the system after their leave date.
- There was no central record that could be used to identify what systems access an individual holds across the Council's systems.
- Data inconsistency across HR and ICT systems made reconciliation of user accounts difficult.

Management Response

1.8 The findings of the report have been accepted by management who have agreed management actions to address them. These included:

- The Active Directory has been linked to the HR system which ensures that 'leavers' recorded by HR are prevented from accessing the Council's systems relying on domain authentication (single sign on is an example of domain authentication), but this leaves some residual risk for systems where domain authentication was not required. This has also resolved in part the data inconsistency between HR and ICT
- The feasibility of role-based access control implementation is being explored; if this is not possible, other appropriate risk mitigations will be determined
- A new simpler 'leaver process' has been put in place and leaver access to accounts dependent on domain authentication, including email, is now revoked at midnight on their leave date
- For the core IT system reviewed, which does not utilise Domain Authentication and holds highly sensitive information, regular reports were to be obtained to monitor appropriate user access