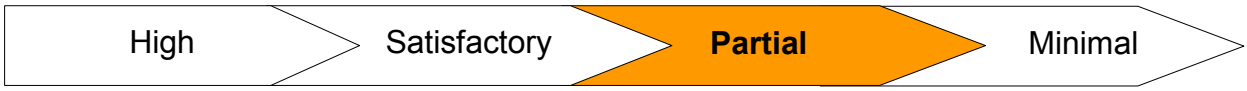
Appendix 2b: Audit Opinion and Summaries

Assurance



Agresso System Access Control

Objective

To assess whether there are adequate arrangements in place for ensuring that at any point in time, individual staff members' access to the functions within the Agresso system is in accordance with the needs of their job role.

Summary

The Council's three overarching IT security policies are of good quality, highlighted to staff when joining the Council and available on the intranet for reference. They should all be reviewed, potentially consolidated and reapproved by the Director of Legal and Democratic Services, who is now the Senior Information Risk Owner. ICT also has an ICT Standard Service Level Agreement (SLA), which details action timeframes for four priorities of request, which does not appear to be widely known. This may explain the higher than expected levels of requests made on or after the dates they should have come into effect.

Line managers are accountable for submitting initial Agresso access, changed access and access revocations requests. As this comes from 'management', the ICT Agresso team take this as the 'authority to action'. However, it is not unusual for requests to be sent by other, sometimes more junior staff members.

A current staff profile can be selected to be copied or a default level of access will be applied. Some evidence was found of inappropriate or incorrect access profiles being applied. In the short term, some management review is needed within ICT to ensure such requests are consistently and accurately processed.

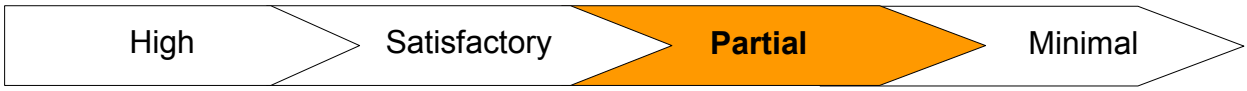
The main concern is that the level of access being granted to staff (i.e. access templates being used) is not clearly linked to employees' job roles. This is an issue which is outside of ICT's direct control and dates back to when Agresso was first implemented. Addressing this in a timely manner would be a significant task. A potential approach would be to tackle this iteratively, focussing on the highest risk areas first. A level of risk would need to be accepted until this work is completed. The process to be adopted for granting, changing and revoking Agresso system access also needs to be documented in some form.

Some ICT staff members and all HR staff have elevated levels of access to Agresso both to carry out administrative tasks and troubleshoot problems. The on-going validity of this needs to be confirmed. In general, this level of access needs to be minimised to situations where it is absolutely required, logged and justified.

Apart from for a small number of ICT staff, access to Agresso is linked to network logins which have appropriate automated enforcement of password length, complexity and expiry. These same standards need to be automatically enforced within the Agresso application.

Appendix 2b: Audit Opinion and Summaries

Assurance



The Agresso Review Group (ARG) is responsible for the development and on-going use of Agresso. It is correctly constituted, has clear Terms of Reference and appropriate membership. ARG meetings are formally managed, with agendas and minutes produced. It should also be involved in approving the 'design' of roles that define the various levels of access to Agresso as well as the employees that are allocated to each. A one off exercise started in October 2016, to confirm all Agresso users have the correct access profile was not completed. It needs to be repeated but taking a different approach, involving operational managers. Once it has been confirmed that all staff access profiles are correct:

- service managers should be asked to confirm every six months, that this remains the case for all the staff that they manage
- relevant staff should be asked to confirm annually, that the design of the templates giving access to their areas remain correct.

The ARG should receive summary reports where significant exceptions in access granted are identified.

Number of actions agreed: 20