Appendix 2d: Audits Revisited

Purpose of these audits

To assess whether the actions agreed in the original audit report have been implemented and are now effectively embedded into the day-to-day operation of the service.

Unit 4 Business World System Access Controls Revisited

Opinion: Partial assurance

Original 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 Unit 4 Business World (U4BW) (formerly named Agresso) system is in accordance with the needs of their job role.

Results

Fully implemented	Substantially implemented	Partially implemented	Not implemented	Closed
9	0	0	8	3

Summary

The Council's three overarching IT security policies still require review and approvals by the Council's Senior Information Risk Owner to ensure they align with good practice and continue to meet the needs of the organisation.

It was not deemed practical to limit requests for new users to managers only. Instead, an alert has been developed within Unit 4 Business World (U4BW) that notifies managers when a new user request has been made and advises them to contact HR if they believe there to be a mistake.

Work has been undertaken to develop user management procedures that make clear the process for granting, amending and revoking access by ICT staff. Further work is needed to develop a monitoring process that gives assurance these procedures are being consistently adhered to. More work is also needed to manage the business' expectations around time for requests to be actioned, and ICT will work with HR to ensure managers have greater awareness around these.

A significant piece of work is needed to address how user access permissions are granted, and this will be achieved in the main through the development of a corporate establishment. This will allow permissions to be driven by job roles with pre-set access profiles linked to that job role, rather than the current practice of copying profiles between individuals, which increases the potential for inappropriate access to be given.

In the short term, work will be undertaken within ICT:

- for existing ICT staff, to review access to particularly risky (e.g. Accounts Payable) or sensitive (e.g. HR) profiles and ensure staff only have this access where it is essential to their role

- to continue issuing new staff with only basic level access unless requests for enhanced permissions are made by line managers.

The HR Service Manager - Operational Services will continue to monitor those with access to the full HR profile on an annual basis.

ICT will continue monitoring the use of profiles not linked to an individual e.g. SYSTEM. Further work is needed to monitor the creation of U4BW profiles:

- not linked to individuals i.e. accounts such as TESTUSER or SYSTEM
- where there is a risk of ghost employees being set up.

Login and password settings have been aligned to the Active Directory for those staff that are not automatically connected to U4BW via their network login.

There remains a need for the Unit 4 Business World Review Group to review the alerts currently set up within U4BW to ensure inappropriate activity within the U4BW modules (e.g. Accounts Payable, Payroll) can be pro-actively identified, minimising the impact on the Council.