

ICT Recommendations update

Contact Officer: Steve Palmer
Telephone: 01895 556033

REASON FOR ITEM

At the last Audit committee, members drew attention to a number of ICT recommendations that had been outstanding for some time. The committee asked that the Council Head of ICT and Business Services attend the next audit committee to explain the steps that were being taken to clear these recommendations.

This report summarises for the Committee the current status of Audit recommendations in the ICT area. It details the recommendations outstanding at the last Audit Committee and the actions that have now been taken to deal with them. Significant progress has been made with all recommendations either implemented or agreed with Internal Audit to be classed as no longer relevant.

While carrying out this exercise the Head of ICT and Business Services has reviewed the ICT approach to recording and processing agreed audit recommendations. Central monitoring of progress and actions is now fully in place with structured liaison and contact points between Corporate ICT and the Council's Internal Audit Service

The Head of ICT and Business Services will be in attendance to answer any questions members may have.

RECOMMENDATIONS

The Committee should note the progress made and to seek any explanations of actions from the Head of ICT and Business Services.

INFORMATION

The information supporting this item is attached as a table of actions.

BACKGROUND PAPERS

Head of Audit and Enforcement update report to this Committee of June 2011

Annexe 1

YEAR	TOPIC	HIGH/MED/LOW	RECOMMENDATION	ACTION & RESOLUTION	STATUS
2007/8	Business Continuity Planning		A well-defined disaster recovery plan, (including satisfactory secondary ICT site) should be provided for ICT back up/disaster recovery	The Disaster Recovery plan was completed in Quarter 1 of 2011. A full generator test scheduled for 31 st August provided an opportunity to test plans and this was successfully achieved. A further test is scheduled for December 2011	Implemented
	Business Continuity Planning		The Head of Resources, Policy & Performance (for Education and Children's Services) should ensure there is a detailed and approved disaster recovery plan in place	Provision is included and was completed in Quarter 1 of 2011.	Implemented The Civic Centre
			All the above have been submitted to and verified by both Civil Protection and Audit colleagues. The majority of these documents having been completed in December 2010 with the current review cycle planned to close in December 2011. A further review will take place post implementation of the ICT Managed Service Tender and Desktop Review tender which will be let by the end of November 2011.		
2008/9	Help Desk	Medium (04/11)	Development of the Configuration Management Database (CMDB) together with the knowledge base and service catalogue and their alignment and integration should be prioritised and agreed.	Report recommended that CMDB and service catalogue integration be prioritised to obtain an accurate snapshot of the network and its components, e.g. Computers, Servers, etc. Since the report was first issued, we have now implemented a new asset management tool, Centennial, which is fully utilised by the ICT team and provides full functionality. This allows the capture and tracking of all software and hardware connected to our network and assists us in ensuring compliance in licensing regulations. The call logging software we use, LANDesk Service Desk provides a knowledge base feature.	Implemented
	Remote Access	Medium	Management should introduce a programme for analysing the logs of remote access sessions in order to identify any inappropriate or unauthorised activity	Provision of remote access is through a Citrix solution. The costs of linking this to an automated process to flag intrusion alerts would include many false positives due to the volume of forgotten passwords, making this neither a pragmatic or cost effective solution. However, we now obtain reports which are manually reviewed to ensure user accounts are still valid.	Internal audit have now agreed this approach is acceptable and have closed the recommendation
	Remote Access	Medium (03/10)	Management should consider obtaining and implementing an intrusion detection	This has previously been considered and the consensus of ICT management and partners with wider industry	Internal audit have agreed to

Annexe 1

YEAR	TOPIC	HIGH/MED/LOW	RECOMMENDATION	ACTION & RESOLUTION	STATUS
			system, together with procedures for checking and acting upon reported attempts at unauthorised access	experience is that the resources required would be disproportionate to the benefits. Since inception, we have met the required standards of the GCSx Code of Connection and that accreditation closely scrutinises both of the mentioned actions. This assurance that any risks are mitigated is further supported by the lack of any breach in our security	close this recommendation
	Ocella Application			Follow up of this audit action was in progress at the time of the last Audit Committee. The recommendation has now been fully implemented	Implemented
	Email Security & Management		Develop and document business continuity arrangements for the E-mail system	Restoration of mailboxes has now been fully tested as part of the Business Continuity plan and the recommendation is complete	Implemented
2009/10	Environmental Services Application M3			This application has now been superseded by Flare, implemented in Dec/ Jan 2011. As such the outstanding actions are no longer relevant	Application being replaced. Recommendation withdrawn
	ICT Disaster Recovery (DR)	Medium (end 10) High (08/10) Medium (07/10) Medium (12/10)	Four recommendations were noted as outstanding in June 2010: <ul style="list-style-type: none"> • Order of Service recovery in a power outage • Disaster Recovery Plan produced • Identify systems for backup • Staff adequately trained in DR procedures 	All four recommendations have been fully implemented, tested, documented and approved by Senior management. These recommendations are closely linked with the Business Continuity plan and will continue to be reviewed and updated in line with this plan to reflect changes and updates to our infrastructure and services we support.	Implemented
2010/11	Hardware Disposals			All recommendations were fully implemented	Implemented
	Software Licensing		The Council should expedite and set a target completion date on the current work to prevent all users from installing any software.	In place. Reduces rights and will prevent unauthorised software installations. However, due to the nature of their role, select individuals require administrator rights and their usage is monitored on a regular basis	Implemented