

Manchester City Council

Audit of Accounts 2009/10
Information Systems Controls - Follow Up Review

November 2009

Final

Contents		Page
1	Executive Summary	2
2	Detailed Findings and Action Plan	5

Information Systems Controls Follow Up Review

1 Executive Summary

1.1 Introduction and scope

This report highlights the key issues arising from our follow up review of the agreed recommendations to be implemented from our previous audit of the Council's key information systems controls, which was reported to the Audit Committee in June 2009.

The objective of this review was to assess whether agreed actions from our previous audit have been implemented, where dates for implementation have been reached, or to determine if adequate progress is being made towards completion of other recommendations that are ongoing.

The findings from our review will also feed into our 2010 Use of Resources assessment, particularly aspects relating to the production of relevant and reliable data and information to support decision making and manage performance.

We will also use the findings from this follow up to scope and inform other information security audits identified as part of the 2009-10 audit plan.

1.2 Key Conclusions

Overall, there has been significant progress in implementing earlier agreed recommendations. Of the fifteen recommendations agreed, we are pleased to report that five have been fully dealt with and significant progress made with others. These include addressing fundamental issues relating to the Council's anti-virus software and the critical security task of patch management.

Key recommendations where significant progress has been made include:

- **Security Management** - following the virus incident in December 2008, the Council signed a contract with Microsoft to assist it, first with the containment, and then the elimination of the Conficker virus. This partnership resulted in a number of risk assessment projects that involved the identification and improvement of security controls over the network infrastructure, Active Directory, and overall ICT operations
- **Anti-virus policy** - the virus incident has been successfully contained and managed by installing standard anti-virus software on all desktops, laptops and servers. The ICT Service has rolled out approximately six hundred Citrix terminals and is expected to deploy two thousand terminals by March 2010. This, with the enhanced anti-virus policy, permits centralised control over security management thus enabling improved control over user access
- **Patch Management** - one of the key reasons why the Conficker virus was able to spread so prolifically across the Council's IT network was due to poor patch management. We are pleased to report that a new patch management strategy has been established that entails the review, testing and deployment of patches to servers and workstations in a timely manner

Information Systems Controls Follow Up Review

- **ICT Service reorganisation** - the ICT Service has been restructured and management and leadership capabilities have also been improved through the recent appointments of a Chief Information Officer (CIO), Head of ICT Operations and Head of ICT Strategy and Change. While the recruitment process is in progress, critical vacant posts within the ICT Service have been fulfilled by contractors. This has enabled the Council to ensure key operations are managed until permanent staff are in post. It is hoped that all identified posts will be filled by end of January 2010
- **Government Code of Connection** - the Council has now achieved compliance with the Government's Code of Connection, which now enables it to have access to the Government's secure extranet. One key aspect of this compliance is the requirement to have in place information security controls that meet a high standard. The Council's policy of increasing the complexity of user passwords for all network accounts, and the implementation of a single sign on capability that removes the need for multiple passwords, has helped with this process and mitigated a number of security risks
- **ICT Strategic Partner** - through a competitive process, the ICT Service has recently engaged a firm - Ernst and Young - to work with it as a strategic partner for two years to assist in the development of ICT plans and operational policies
- **ICT Disaster Recovery** - an initial draft of the ICT Disaster Recovery Plan has been compiled although this requires further development. An alternative site has been identified to host the data centre to remove the need to use the existing facilities at the Town Hall. The city centre location and the basement area are not ideal places for such recovery sites and we welcome the new arrangements. The move of the data centre is a key part of the Council's revised disaster recovery planning that is expected to be completed and tested by March 2010
- **Network monitoring** - The ICT Service has initiated the procurement of a system monitoring solution that will track and monitor ICT assets, review security event logs, report system performance, and help with software licence compliance. This software will enable improved control over the ICT estate. The ICT Service expects to procure the solution by end January 2010.

However, our review did identify a number of areas where progress with agreed recommendations has not been as rapid as others. This has resulted in agreed target dates not being met. We acknowledge that this is in part a result of the volume of work that was required and commend the effort that the ICT Service has put into dealing with a number of difficult issues. However, there remain a number of key controls that require decisive action to ensure that all risk areas are being actively managed. These include:

- **IT asset management and security monitoring** - we recommend that Management should agree and procure the system monitoring solution as a matter of priority to ensure its prompt and timely implementation
- **Network administrators** - our review found that that there are still multiple administrator accounts assigned to one individual. We recommend a full documented review of all network administrators to assess the business rational behind multiple accounts that allow privileged access
- **User Account Management** - our review highlighted that the leaver and transfer process has not yet been fully established. This increases the risk of improper use of active network accounts belonging to employees who have left or have changed roles. We recommend that procedures should be developed by ICT in conjunction with the

Information Systems Controls Follow Up Review

Human Resources department to actively manage changes as required. The Council should also perform regular reviews of users to identify inactive accounts and access levels

- **Network Penetration Testing** - although we accept that the imminent introduction of regular penetration testing, as required by the Government Code of Connection, will improve overall management control over network vulnerabilities, we are of the view that key server issues that are identified on a daily operational basis should be reported to ICT senior management to ensure risks are captured and mitigated appropriately. This process should be improved by the procurement of the monitoring solution.
- **Disaster Recovery Planning** - while an initial draft plan has been compiled, we recommend that the plan should be improved by instituting a clear definition of a minimum acceptable recovery configuration for key business areas and their systems. A Council-wide testing strategy should be prepared in advance to ensure the amalgamation of the IT recovery plans with the overall business continuity plan
- **ICT policies** - our recommendation to develop centralised ICT policies as well as updating key security policies has been deferred to prioritise the implementation of strategies that ICT Management has deemed more critical. We recognise that this area has not been deliberately disregarded. However, we would encourage ICT Management to ensure this issue is now given greater prominence, particularly in light of the number of new ICT staff starting with the Council in the coming months.

1.3 Responsibility of IT Management

This report has been discussed with the Chief Information Officer, Head of Operations and Head of Strategy and Change.

Our work did not encompass a detailed review of all aspects of the systems and controls in place, and cannot be relied upon necessarily to disclose all weaknesses.

This report has been prepared solely for use by the Council and should not be used for any other purpose. We assume no responsibility to any other person.

1.4 The way forward

We have made a number of recommendations which are set out in the attached action plan alongside the original and updated detailed findings.

1.5 Acknowledgements

We would like to record our appreciation for the positive co-operation and assistance provided to us by the ICT department at the Council during the course of our audit.

Grant Thornton UK LLP

November 2009

Information Systems Controls Follow Up Review

2 Detailed Findings and Action Plan

In the following section, **high** priority recommendations correspond to fundamental control risks; and **medium** priority recommendations apply to control risks that exist and require attention.

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
<p>1. A server change policy should be formalised to cover all stages of the server change process. This policy should outline the life cycle that each server change must follow. The life cycle must incorporate:</p> <ul style="list-style-type: none"> • Formal documentation of change request, including assessment of changes; • Formal documentation of test scripts and test results for all changes; and • Formal sign-off from IT 	<p>High</p>	<p>A Patch Management Strategy is to be developed within the ICT Service, following initial improvements made by Microsoft. The scope of this strategy will include servers and the desktop / laptop environment. This strategy will ensure that all changes are fully tested and documented.</p> <p>Strategic Head of ICT (Steve Park) October 2009</p>	<p>Status: Completed</p> <p>There is an existing overall change management process that governs customer-initiated changes to systems.</p> <p>The ICT Service implemented a workstation patch management process in July 2009 incorporating the use of Microsoft Windows System Update Server (WSUS) to obtain the latest patches that will be evaluated during weekly patch review meetings. The WSUS documentation covers the patch management process incorporating evaluation of what patches are necessary. Roles to assess and review patches are assigned to the Security Team with the Server or Workstation Teams responsible for implementing patches. Each team is responsible, following the guidance of the Security Team, for improving assessed and reviewed patches. Testing of new patches is performed</p>	

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
<p>management prior to release into production environment.</p> <p>This policy should be applied to all operating systems used by the Council.</p>	<p>Revised priority: Medium</p>		<p>by the ICT Service and carried out over a weekly test programme. Patching is then carried out across the estate, site by site. Weekly minutes of patch review meetings capture approvals as well as issues from testing. There is an email distribution list to inform senior management of imminent Microsoft server patch releases for the month.</p> <p>Citrix servers are not currently managed as part of the WSUS configuration but governed through a manual process. Processes for patch review, deployment into the test environment, monitoring, deployment into the live environment and updates to the automatic scripts for all new server builds are in place but not fully documented. This documentation is expected to be completed by end of December 2009.</p> <p>Updated Recommendation: We recommend that ICT Management ensure target deadlines to complete process documentation are met so that controls are consistently applied across the ICT department. This is important particularly with new ICT support staff joining the Council. Process documentation is critical but even more so in a changing environment such as that being experienced by the Council.</p> <p>There is a monthly management report provided to give high-level feedback on the Microsoft server patches implemented and any outstanding risks. However, this does not include the Citrix servers. No formal management reporting is in place for Citrix server patches.</p>	<p>Although a manual process, Citrix server patches are kept up to date. Focus in the last 4 months has been on patching non-citrix servers to remediate critical vulnerabilities. Citrix server management will be incorporated into the broader Server Patch Management Process.</p> <p>Target Date: April 2010</p>

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
			<p>Updated Recommendation: We recommend a similar process for management reporting, i.e. email distribution and monthly reporting, be implemented for Citrix server patches. Senior ICT Management team members will therefore be aware of the patches that will be applied to the Citrix servers, and will receive assurance that patches are evaluated/approved and tested before deployment.</p>	<p>Management action, as above Target Date: April 2010</p>
<p>2. Although we understand that IT is currently still in the process of recovery, we recommend that measures are taken to ensure that all PCs are cleaned and installed with the correct up-to-date anti-virus software. We are aware IT are in the process of replacing desktops with Citrix terminals. If this is considered a solution to the virus problem, we recommend IT make this a matter of priority.</p>	<p>High</p>	<p>An ICT Security Policy is to be refreshed and re-launched that will include the Council's approach to anti-virus software and how it is installed across the estate. This policy will cover not just PCs but mobile media and servers.</p> <p>The rollout of thin-client (Citrix) PCs remains a priority for the ICT Service and these will be targeted where performance problems are causing the highest level of disruption to service delivery.</p> <p>Strategic Head of ICT (Steve Park) October 2009</p>	<p>Status: Completed</p> <p>Following the virus incident in December 2008, workstations have been 'locked down' to disallow the use of removable media, which was how Management believes the virus was introduced to the Council's network.</p> <p>Kaspersky Anti-Virus (KAV) has been comprehensively deployed across all desktop and laptop computers and servers. The Citrix server farm continues to be protected using Symantec anti-virus software. Both are configured to obtain regular virus definition updates from Kaspersky and Symantec and regularly push updates to connected workstations. Laptops for mobile users are manually configured to obtain updates from Kaspersky through the Internet to ensure coverage when not connected to the network.</p> <p>The management information that is obtained on a daily basis shows very low levels of virus activity, and is used to target cleansing or Citrix terminal replacement actions.</p>	

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
			<p>To improve overall security and deal with the virus the ICT Service has deployed nearly 600 Citrix terminals since May 2009. These have included 110 deployments in the Children's Department where the virus was causing most disruption to the Council.</p> <p>The targeted deployment of the Citrix terminals has involved complex changes to several applications to ensure they are accessible through a Citrix environment. This caused a trade off between targeting areas of high virus activity and the pace of deployment, which was lower than anticipated. However, it is now expected that 1,000 Citrix terminals will be deployed by December 2009 and a total of 2,000 by March 2010.</p> <p>However, the ICT Security Policy has not been refreshed and re-launched to include the Council's approach to anti-virus software and how it is installed across the estate.</p> <p>Through a competitive process, ICT Management have engaged Ernst and Young as a strategic partner for two years to assist in the development of strategic ICT plans and operational policies, including the refresh of the IT Security Policy.</p> <p>Updated Recommendation: We recommend that the IT Security Policy is updated as soon as the partnership with Ernst and Young comes into effect.</p>	<p>The Corporate ICT Security Policy will be re-written in light of lessons learned in 2009, latest best practice and planned deployment of new technology in</p>

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
				2010. This will be a priority action, along with the Corporate ICT Desktop Policy, with E&Y. Target Date: April 2010
<p>3. We recommend that the Council performs a review of IT assets as a matter of priority in order to establish the number of different types of IT asset across the Council, including details of specification, software and hardware installed.</p> <p>We understand that IT is in the process of replacing selected desktops with Citrix terminals, which can coincide with the IT asset review.</p> <p>If possible, it would be preferable for IT to be able to take ownership of IT assets across the Council.</p>	High	<p>The ICT Service has recently recruited an individual to focus on asset management.</p> <p>Strategic Head of ICT (Steve Park) October 2009</p> <p>The ICT Service will be compiling a business case and if supported, procuring a system monitoring solution that will log and track the use of all ICT hardware across the Council, including the software used and associated licences.</p> <p>In line with the ICT Strategy, the ICT Service will be taking ownership of all ICT,</p>	<p>Status: Completed</p> <p>The individual assigned responsibility for asset management is a contractor although there are plans to recruit a permanent member staff to fill the post by January 2010.</p> <p>Status: Ongoing</p> <p>ICT has initiated the procurement of a system monitoring solution, and is awaiting demonstrations from a number of software vendors based on an Invitation to Tender (ITT). Technical specifications have been prepared by the ICT Service. The aim is to procure the system monitoring software by December 2009 and implement throughout 2010. The business case has been documented but no budget has been agreed. The Council is awaiting the results of the response to the ITT before it decides on the solution.</p>	

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
<p>The existing arrangements are disjointed. This will ensure that any new IT asset purchase is controlled and managed through IT.</p>		<p>including staff. The staff consolidation will be the first stage of this process.</p> <p>Strategic Head of ICT (Steve Park) October 2009</p> <p>The deferred Internal Audit on IT assets has been included in the 2009/10 Internal Audit Plan. Timing has to be agreed with the ICT service but it is expected this review will be completed by December 2009.</p> <p>Head of Audit and Risk Management (Tom Powell) December 2009</p>	<p>Staff consolidation is expected to be completed by the end of January 2010 when recruitment to the newly created posts is to be finalised.</p> <p>Although delays are not envisaged as advertisements have been published, there is a risk that not all posts will be successfully recruited to at the earliest opportunity.</p> <p>Status: Completed</p> <p>ICT has recently received the draft report from Internal Audit on IT Asset Management. At the time of our follow up, Management was in the process of providing responses.</p>	
<p>4. A full review of all network administrators, including domain and delegated administrators should take place.</p> <p>We are led to believe that there should not be any local administrators. All creation, modification and</p>	<p>High</p>	<p>The work described in the recommendation has already commenced.</p> <p>Strategic Head of ICT (Steve Park) July 2009</p> <p>The consolidation of the ICT</p>	<p>Status: Ongoing</p> <p>The ICT Service has restricted administrator rights to all workstations through group policies within the MCC domain. Any requests for access must be registered through the ICT Service Desk and are required to be supported by a business case to ensure an audit trail.</p> <p>However, no management report is available to provide evidence that a full review of network administrators has</p>	

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
<p>removal of leavers is centralised within IT. If this is the case, all local administrators should be removed from the network.</p> <p>Administrator rights should be restricted to personnel which require such access as part of IT operational duties. Such rights should be formally documented and approved by a senior member of IT management.</p>		<p>Service will work toward this recommendation being implemented.</p> <p>Strategic Head of ICT (Steve Park) October 2009</p>	<p>taken place. Our review of the list of domain administrators discloses the following:</p> <p>Previously - 51 domain administrators with some users have up to 3 domain administrator accounts.</p> <p>Update - 46 domain administrators, 22 of which belong to staff in the ICT Service. We still noted a number of users having 2 to 3 domain administrator accounts.</p> <p>Updated Recommendation: We recommend that Management evaluates the need for multiple domain administrator accounts. While we expect administrators to have up to 2 accounts, we expect one of the accounts to be given lower privileges as this would be for day-to-day use.</p>	<p>Agreed. It is expected that this will be addressed by reducing the number accounts available to staff. Target Date: January 2010</p>
<p>5. We recommend that IT management complete the IT centralisation project and develop centralised IT policies, to cover:</p> <ul style="list-style-type: none"> • Setup/modification and removal of user access for the network and applications; • Program change 	<p>High</p>	<p>The consolidation of the ICT Service remains a key objective for the Council. The process is underway to transfer staff into the ICT Service as a first stage of consolidation. This will be followed by consolidated, single policies that are applied consistently across the</p>	<p>Status: Ongoing</p> <p>Management has engaged Ernst and Young as a strategic partner for the ICT Service to assist in the development of strategic ICT plans and operational IT policies. A preliminary plan of action based on strategic initiatives with timelines is expected to be completed by mid-December 2009.</p>	

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
<p>requirements for the application systems development process that includes quality assurance, testing, and migration to the 'live' environment;</p> <ul style="list-style-type: none"> • Software development, acquisition and implementation policy; • Virus management policy; • Firewall policy; • Data Security policy; • Domain policy (including audit policy, password policy and account lockout policy); • System backups and recovery policy; • Disaster Recovery and Business Continuity policy; and • Physical Security policy. 		<p>Council and then the technology itself.</p> <p>Strategic Head of ICT (Steve Park) March 2010</p> <p>This will be implemented as part of the consolidation of the ICT Service.</p> <p>Strategic Head of ICT Steve Park October 2009</p>		

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
<p>Once developed, the policies should be approved by senior management and applied across the Council.</p>				
<p>6. Management should standardise the leaver and transfer process and ensure that this is applied consistently across the Council.</p> <p>The Council should develop formal procedures to ensure IT are notified of leavers on a timely basis by Personnel, and for IT to ensure that network logins and SAP accounts are deleted or suspended on or soon after an employee's date of departure.</p> <p>IT should develop a regular process to identify inactive users, ensure that they are still required and disable any inactive accounts.</p>	<p>High</p>	<p>A revised start and leaver process is to be developed and implemented in the ICT Service. This will be linked in with Personnel, Finance and Service Managers.</p> <p>Strategic Head of ICT (Steve Park) November 2009 Management information will be made available that will indicate user accounts that have remained inactive and are therefore candidates for deletion.</p> <p>Strategic Head of ICT (Steve Park) November 2009</p>	<p>Status: Ongoing</p> <p>The starter process has been and implemented. However, formal documentation to support this has not been developed. The process is instigated by HR through the Notes database where another member of staff within the same department who would have the same level of access is selected and their access levels are 'copied' to the new account. This action triggers an automatic logging of a call to the service desk system. This results in the creation of the network user account. However, there is no evidence that access given to staff to other systems that has been separately requested (not default to the role against which the base- lining takes place) is being assessed before a user account is created, for example remote access. This poses the risk that inappropriate access rights may be given to the new user.</p> <p>Updated Recommendation: We recommend that a list of access levels that require individual authorisation are identified. The list should be issued to the Service Support team for reference. This will help ensure that any separately requested access to systems is not copied over from the template account and that approval is properly obtained for</p>	<p>A start \ leaver \ user access amend process will be developed that will include the deletion of inactive accounts. ICT management note the risk posed by the this issue, however to date</p>

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
<p>The Council should also implement a process for periodic reporting of all active network users and their access levels. This report should be communicated to the relevant managers within the Council who should confirm access rights are consistent with the department's requirements.</p>			<p>the system as required.</p> <p>The leavers process is also initiated by HR through the Notes database. However, no automatic logging of service desk calls has yet been implemented. This increases the risk of leavers' accounts remaining active and subjected to unauthorised use. ICT Management plans to revise this process by December 2009.</p> <p>Our review found that no progress has been made with regard to the transfer process. ICT Management expects to complete this by end of March 2010.</p> <p>Status: Ongoing</p> <p>The Windows Server team does not perform a regular review of inactive accounts. However, accounts for external consultants are set up with a specific end date. The single sign on process, although having many benefits, relies on good account management. This becomes critical as a compromise of the account may lead to unauthorised access of systems. The existing process for leavers and the absence of a regular review of accounts and access rights increases risk that inappropriate accounts or access rights remain undetected. Such accounts are at risk of being subject to unauthorised use.</p> <p>Updated Recommendation: We reiterate our original recommendation to implement a formal and regular process to review users and access. This should be done as a matter</p>	<p>resource has been prioritised on more serious threats. For starters and leavers Target date: March 2010</p> <p>To address the much complex process of account transfer process this is linked to several other processes and will be addressed following starters and leavers. Target Date: June 2010</p>

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
			of priority.	Management response is as above. Target Date: March 2010. Target Date: June 2010
<p>7. The Council should prepare an action plan to ensure that recommendations provided in the penetration testing report are implemented and resolved within a defined timescale. Responsibility of each action should be formally agreed and assigned.</p>	<p>High</p>	<p>The results of the external penetration test are being fed into a delivery plan for the service for the next 12 months. Some of the key vulnerabilities highlighted in the penetration test results have already been addressed as part of the ICT Service response to the virus.</p> <p>Strategic Head of ICT (Steve Park) March 2010</p> <p>A formal response to the Internal Audit report will also be provided to ensure that all the identified areas for development are addressed.</p>	<p>Status: Ongoing</p> <p>The penetration exercise undertaken by a third party in 2008-09 found that most vulnerabilities related to patches not being updated. The IA report has been finalised after receiving responses from ICT Management.</p> <p>There are critical internal servers and eight critical external servers and these were tested as part of the IA review. WSUS is used to manage all patches. Four of these internal servers have updated patches. Three internal servers are in the process of remediation while no work has been performed on the remaining servers. There are a number of possible explanations for this:</p> <ul style="list-style-type: none"> • The server is offline during the scan; • The server has been removed or replaced and not included in the scan; or • The server is in a different OU or sub-OU. <p>The external servers are maintained by third parties and</p>	

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
		<p>Strategic Head of ICT (Steve Park) July 2009</p>	<p>existing requests to comply with patch management process and testing through Microsoft Baseline Security Analyser (MBSA) were noted.</p> <p>There is a risk that some critical servers are not yet fully patched because of the reasons stated above. The monthly management report on Microsoft server patches does not highlight the risk involving servers that are not detected by WSUS.</p> <p>Updated Recommendation: We recommend that the monthly management report includes the reporting of risk of servers not detected and potentially not patched by WSUS.</p>	<p>This will be included in monthly management reports, facilitated eventually by the network monitoring solution. Target Date: January 2010</p>
<p>8. We recommend Management take measures to reassess the vacant roles and the ICT security requirements of the Council as soon as possible, in order to ensure that all of the required IT security roles are undertaken and achieve a clearer distinction between IT security management and IT operations.</p>	<p>High</p>	<p>Additional staff have recently been added to the Information Security team on a temporary basis to relieve the need for operational and security work to be undertaken together. The separation in duties will be formalised through the ICT Service redesign that will be complete by the end of September.</p> <p>Strategic Head of ICT</p>	<p>Status: On-going</p> <p>The staff consolidation is expected to be completed by end of January 2010. The revised ICT restructure provides distinction between IT security management and IT operations.</p> <p>The ICT Service has been restructured to remove siloed functions, inherent single points of failure, and to provide adequate levels of support, i.e. in and out of hours.</p> <p>Management and leadership capabilities have been improved through the recent appointments of a Chief Information Officer, Head of ICT Operations and a Head</p>	

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
		<p>(Steve Park) October 2009</p> <p>The ICT Security team will be restructured as part of the wider service restructure, specially to remove single points of failure. The recent addition of temporary staff has relieved some of this pressure.</p> <p>Strategic Head of ICT (Steve Park) September 2009</p>	<p>of ICT Strategy and Change. IT operations and IT Security fall under the command of the Head of ICT Operations, led by different Operations Managers. The Head of Strategy and Change is focused on developing and prioritising the ICT Service roadmap and developing relationships with customers in service areas across the Council.</p>	
<p>9. We recommend establishing and formalising a detailed disaster recovery process for the IT systems, clearly defining what areas are to be given priority in the event of a disaster and providing coverage of the high priority systems. Once developed, the plan should be integrated with the overall business continuity plans for the Council and approved by senior</p>	<p>High</p>	<p>The ICT Service Business Continuity and Disaster Recovery processes will be refreshed and will target critical systems. This will be met in part by the completion of the Server Virtualisation Project.</p> <p>Strategic Head of ICT (Steve Park) November 2009</p>	<p>Status: Ongoing</p> <p>The ICT Service now has an initial draft of a Disaster Recovery (DR) plan. This plan will be further developed in January 2010 in conjunction with the strategic partner to ensure it is integrated with service contingency plans across the Council.</p> <p>The Business Impact Analysis (BIA) will be conducted to inform the future design requirements and backup strategies. We found that the Civil Contingency Unit performed this recently. However, results of this exercise were not considered effective as assessments were one-sided and most systems were considered critical. This resulted in the absence of a defined minimum acceptable recovery configuration for</p>	

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
<p>management. It should then be communicated to all relevant personnel.</p> <p>The disaster recovery plan needs to be reviewed and tested on a regular basis (minimum of once every 12 months) to ensure that recovery procedures and responsibilities are sufficient and up to date.</p> <p>In addition, IT should also perform an assessment of the impact of the Town Hall refurbishment on the BX45 suite and ensure that any risks are mitigated or minimised in order to ensure physical security and environmental controls over the servers are not jeopardised.</p>			<p>key business processes within the plan.</p> <p>Also, there is no outline of the test strategy to be used for the DR plan once completed.</p> <p>Updated Recommendation: We recommend the following to be considered during further development of the DR Plan:</p> <ul style="list-style-type: none"> • Define a minimum acceptable recovery configuration for key businesses and systems; and • Outline a testing strategy. <p>An alternative site has been identified to host the data centre away from the city centre. This site has been obtained in conjunction with the Manchester Digital Development Agency (MDDA) and offers improved environmental conditions, security and recovery capabilities. The new data centre is a key part of the Council's ICT disaster recovery planning. It is expected that the data centre will be fully operational by March 2010.</p> <p>We understand that the Town Hall refurbishment will commence after the relocation of IT facilities to the new centre.</p>	<p>The points are noted and will be incorporated into the next development of the ICT DR Plan that will be undertaken in conjunction with E&Y. Target Date: April 2010.</p>
<p>10. We recommend that IT completes the revision and agreement of the Information Security Policy and also develops an IT Acceptable Use Policy.</p>	<p>Medium</p>	<p>The acceptable use element of the Email Policy will be refreshed in association with Corporate Personnel. This process has already begun following an Internal Audit</p>	<p>Status: Ongoing</p> <p>The Acceptable Email Usage policy has a revised date for completion - end January 2010 - due to other issues being given priority.</p>	

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
<p>The new policy should provide users with an understanding of the policy, its purpose, guidelines for following security practices, and definitions of their responsibilities.</p> <p>All users should be required to acknowledge their acceptance of the new policy and renew acceptance with any revision of the policy. Due to the number of users we would consider it practical to obtain and record user's acceptance of the policy as part of their login to the network.</p>		<p>review of email in 2008/2009</p> <p>Strategic Head of ICT (Steve Park) November 2009</p>		
<p>11. The password policy should be updated to include:</p> <ul style="list-style-type: none"> • password complexity • re-login after periods of inactivity. 	<p>Medium</p>	<p>All of the recommendations listed will be picked up under the ICT Service's approach to achieving compliance with the requirements of Government Connect.</p> <p>Strategic Head of ICT</p>	<p>Status: Completed</p> <p>The Council was awarded its certification of compliance with the Government's Code of Connection in October 2009.</p> <p>In line with the objective of providing secure and safe ICT systems, and to achieve compliance with the Code of</p>	

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
<p>This policy should apply to all network user passwords as well as critical business applications.</p>		<p>(Steve Park) November 2009</p>	<p>Connection, the ICT Service has increased the complexity of user passwords. In August 2009, complex passwords were enforced for all network accounts in the MCC domain.</p> <p>All new passwords must contain at least 3 out of 4 character types (upper-case letters, lower-case letters, numbers and extended characters); must not contain the username or parts of the full name that exceed two consecutive characters; cannot be re-used within 20 password changes; must be a minimum of 8 characters in length; must be changed every 60 days; and have to be used for at least 2 days before they can be changed.</p> <p>We noted that screensaver passwords are not set within the Active Directory. Without re-login after a period of inactivity, this exposes unprotected workstations within the Council to unauthorised use.</p> <p>Updated Recommendation: We recommend the screensaver password is enabled within the domain security settings to enforce users to log in again after 15 minutes of inactivity.</p>	<p>The recommendation is agreed. Screensaver passwords will be activated to force a re-login after 15 mins. Target Date: January 2010.</p>
<p>12. System and security event logs should be reviewed and evaluated on a regular basis. The</p>	<p>Medium</p>	<p>The reviewing of event logs will be within the scope of the procurement of a system monitoring solution that will</p>	<p>Status: Ongoing</p> <p>ICT has initiated the procurement of the system monitoring solution and is awaiting demonstrations from</p>	

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
<p>procedure should be formalised and the outcome of reviews should be documented.</p> <p>For a review to be effective it is useful to identify what normal network activity is as this can be filtered out to facilitate the review.</p> <p>Due to the log volumes, IT may consider use of specialist tools to assist with filtering and monitoring.</p> <p>We suggest a documented review of unauthorised access to the network as a minimum.</p>		<p>target specific logs for specific high risk activity. This will include filtering as per the recommendation.</p> <p>Strategic Head of ICT (Steve Park) November 2009</p>	<p>Computerland, ICT's current Technology Partner. ICT expects to procure the system monitoring products by December 2009 and implement the system throughout 2010.</p> <p>Present controls over security monitoring involve the enabling of audit logs which are kept for 60 days. These are used for investigation purposes in the event of security incidents.</p> <p>From a review of audit policy settings, we noted that no auditing is defined for account management events such as:</p> <ul style="list-style-type: none"> • a user account or group is created, changed, or deleted • a user account is renamed, disabled, or enabled. • a password is set or changed. <p>Updated Recommendation: We recommend that ICT Management set this to "Success, Failure" to help determine any unauthorised changes which could indicate mistakes by an administrator or deliberate attacks.</p>	<p>Currently log 'success' but not 'failures'. These will start to be logged: Target Date: Dec 2009</p>
<p>13. A formal procedure should be in place to ensure that remote access is authorised by senior management within the Council directorates.</p> <p>Management may consider nominating users throughout the Council</p>	<p>Medium</p>	<p>13. A 'Secure Remote Access to Council Systems' procedure is in place and this requires approval by line management.</p> <p>14. The ICT Service has now removed dial up access. Access is now via the Citrix</p>	<p>Status: On-going</p> <p>The process is now being managed centrally and requires checks of authorisation via a line manager's signoff. The form bearing this signoff is scanned and stored. However, we sampled a random four such requests and found that the related scanned forms for two of these were not available. Another form did not bear the line manager's signoff. This indicates that the process may not be</p>	

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
<p>who may approve remote access requirements and ensure IT check the validity of requests.</p> <p>14. IT should disable all dial-up remote access users as an immediate measure and replace any users still using this method with either VPN access or Citrix Access Gateway.</p>	<p>Medium</p>	<p>Access Gateway (CAG) or via the VPN. The ICT Service remove access strategy is to have all staff access the network remotely using the CAG.</p> <p>Strategic Head of ICT (Steve Park) November 2009</p>	<p>operating consistently.</p> <p>Furthermore, we found that there is also no formal and regular process to review remote access accounts to identify accounts for deletion.</p> <p>Updated Recommendation: We recommend the ICT department performs a further review of the remote access authorisation process to gain better assurance that this control is operating effectively.</p> <p>We also recommend that ICT Management implements procedures to regularly review remote access accounts to ensure that only existing authorised users are granted remote access.</p> <p>Status: Completed</p> <p>The current network diagram, dated November 2009, shows that no dial-up access is provided. Present access methods include VPN and Citrix Access Gateway (CAG).</p>	<p>Agreed. A review of remote access authorisation will be undertaken. Target Date: January 2010</p> <p>Agreed. As part of the review, a procedure will be implemented that regularly reviews remote access. Target Date: January 2010</p>
<p>15. We recommend a review of the life cycle for software licences, including their purchase, installation, reallocation and reconciliation. Although it is acceptable for different members of staff to be responsible for</p>	<p>Medium</p>	<p>The ICT Service will be compiling a business case and if supported, procuring a system monitoring solution that will log and track the use of all ICT hardware across the Council, including the software used and associated licences.</p>	<p>Status: Ongoing</p> <p>A Configuration and Licensing Manager's post has been created within the new structures. This post is hoped to be filled by January 2010.</p> <p>The Council will utilise the proposed monitoring system to manage its software licensing arrangements.</p>	

Information Systems Controls Follow Up Review

Original Recommendation	Priority	Original Management Response	Update as of 03 November 2009	Management Response and Target Dates
<p>different licences, IT needs to clearly establish which staff are responsible for each stage of the life cycle. This should be centrally documented and managed by a small number of staff. Management may also consider taking measures to restrict users to being able to install their own software. This may also coincide with the removal of local administrators (see also recommendation 5)</p>		<p>This system will provide enhanced management information that will enable a more effective policy to be administered regarding software licences.</p> <p>Software licence management posts will be included in the new ICT Service Restructure.</p> <p>Strategic Head of ICT (Steve Park) November 2009</p>		



www.grant-thornton.co.uk

© 2009 Grant Thornton UK LLP. All rights reserved.

"Grant Thornton" means Grant Thornton UK LLP, a limited liability partnership.

Grant Thornton UK LLP is a member firm within Grant Thornton International Ltd ('Grant Thornton International'). Grant Thornton International and the member firms are not a worldwide partnership. Services are delivered by the member firms independently.

This publication has been prepared only as a guide. No responsibility can be accepted by us for loss occasioned to any person acting or refraining from acting as a result of any material in this publication