



Manchester City Council

Audit of Accounts 2009/10
Information Security Management

April 2010

Information Security Management 2009/10

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

This report is provided on the basis that it is for the Council's information and usage only and is part of a continuing dialogue between the Manchester City Council and us. For this reason, we do not consider it appropriate for the report to be made available, in part or in full, to third parties without our written prior consent. Nor do we accept responsibility for any reliance that third parties may place upon the report.

Information Security Management 2009/10

1 Executive Summary

1.1 Introduction

As part of our 2009-10 audit plan we identified and agreed with management the need to perform a review of information security arrangements at the Council.

The review was conducted as part of our normal audit planning procedures, and informed our 2009-10 Use of Resources assessment, specifically in relation to:

KLOE 2.3: Does the organisation promote and demonstrate the principles and values of good governance?

1.2 Scope of the review

The review focused on the Council's overall information security management arrangements.

The objective of the review was to assess the existence and maturity of information security management arrangements to determine whether or not:

- an approach and framework is in place for designing, implementing, monitoring, maintaining, and improving information security consistent with the Council's risk management culture
- there is visible support and commitment from all levels of management
- an information security policy is in place with clear objectives and activities that are aligned with corporate objectives
- there is an understanding of information asset protection requirements achieved through the application of a formal information security risk management system, for example, ISO/IEC 27005
- there is an effective information security awareness, training and education programme that informs all employees and other relevant parties of their information security obligations set forth in the information security policies and standards
- there is an effective information security incident management process
- there is a measurement system used to evaluate performance in information security management and feedback suggestions for improvement

1.3 Background

The Council has engaged Ernst and Young (E&Y) to work with it as a strategic partner for two years to assist in the development of ICT plans and operational policies, including those in the area of security. E&Y consultants commenced their work late January 2010 and are currently involved in establishing governance structures for IT projects. We acknowledge that the planned work performed as part of the Council's strategic partnership will address a good many of our recommendations. However, the timescales for doing so are as yet unclear.

Since the virus incident in December 2008, patch management and anti-virus management processes have been made stable for the Windows servers and workstations within ICT's remit. These processes are performed by an IT Security team within the ICT operations, which is also responsible for managing firewalls and proxy servers. However, an Internal

Information Security Management 2009/10

Audit report has provided 'limited assurance' following a review of security arrangements across the Council as 'there are significant areas for improvement in key areas of the systems of control, which put the system/process objectives at risk'. Two critical issues were identified in the Internal Audit report issued in March 2010 relating to the lack of anti-virus installation on machines found on Council domains (not managed by ICT) and usage of a generic account to administer the Revenue and Benefits database. A number of other significant issues were raised relating to the lack of active patching and inadequate security configuration settings of the Unix servers and the lack of resources within the IT Security team.

There are a number of ongoing projects that are aimed at improving security, for example the implementation of a system monitoring tool. However, despite recruitment drives to secure resource vacancies remain within the ICT department, including those with a remit for security.

1.4 Conclusions

The existing information security policies were developed based on a best practice information security control framework. However, these policies are now out of date and no longer reflect the ICT's evolving organisational restructuring and the technologies utilised.

We have identified a number of areas where action is required to improve existing controls:

- **Issues from our previous audit** Issues arising from the follow up audit in November 2009 around user account management, audit policy settings, and remote access are still outstanding despite having target dates for completion of December 2009 to March 2010. We understand that the delays have been exacerbated by competing commitments and the lack of success in recruiting staff.
- **IT Security Governance** - an IT security team is in place within ICT, which manages the day-to-day network security including patch management, the rollout of anti-virus updates, and the management of firewall and proxy servers. However, there is a lack of clarity around which senior manager oversees these functions. ICT management needs to ensure that plans to firm up ICT governance structures are followed through, specifically with regard to the formal establishment and designation of information security responsibilities.
- **IT Security Policies and Awareness** - security policies have not been updated since they were approved and implemented circa 1997. Furthermore, Council arrangements over the induction process for new starters are not robust. ICT management has a project in place that will update the policies to include significant changes within ICT. We recommend that as part of this process a review is performed of the existing induction and staff awareness programmes for information security.
- **Incident Management Team** - staff from across ICT are pulled together to deal with incidents and problems, as required. A proposal has been made for the establishment of a dedicated team reporting to the Operations Manager. However, at the time of our audit these plans had not been outlined clearly. We support the creation of such a team and would recommend that this is dealt with as a matter of priority.

Information Security Management 2009/10

1.5 Responsibility of IT Management

This report has been discussed with the Chief Information Officer.

Our work did not encompass a detailed review of all aspects of the systems and controls, and cannot be relied upon necessarily to disclose all weaknesses or to include all possible improvements in internal control that a more extensive special examination might develop.

1.6 The way forward

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

1.7 Acknowledgements

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

Grant Thornton UK LLP

April 2010

Information Security Management 2009/10

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.

Matter arising	Recommendation	Priority	Management Response	Officer Responsible and Implementation Date
<p>1 IT Security Governance An Information Security Forum (ISF) with representation from Corporate Human Resources, the City Solicitor, Internal Audit and the ICT was established. However, this body has not met since 2008 and is not operating as intended, although it has not been officially disbanded.</p> <p>Our queries with Ernst and Young regarding the proposed ICT governance structures disclose that the Design Authority will take responsibility for security. However, the remit and membership of this body has not yet formally established.</p>	<p>We recommend ICT management ensure that plans to firm up ICT governance structures are followed through, specifically the formal establishment and designation of information security responsibilities.</p>	<p>Medium</p>	<p>Agreed</p> <p>An Information Management Board has been discussed with several senior managers in MCC, including the potential terms of reference.</p>	<p>Chief Information Officer (Steve Park)</p> <p>May 31 2010</p>
<p>2 IT Security Policies and Awareness During our review, we noted that: a Security policies have not been updated since they were formally implemented in 1997/08, to include changes in ICT organisation and</p>	<p>We recommend ICT Management update the policies to include significant changes to the structure as well as the introduction of new technologies within ICT. We also recommend ICT and Council Management</p>	<p>Medium</p>	<p>Agreed</p> <p>An Information Security Policy Framework will be available that</p>	<p>Chief Information Officer (Steve Park)</p> <p>Initial draft April 30 2010</p>

Information Security Management 2009/10

Matter arising	Recommendation	Priority	Management Response	Officer Responsible and Implementation Date
<p>technologies used..</p> <p>Without formal reviews/updates, there is no assurance of the policies' continuing suitability, adequacy, and effectiveness.</p> <p>b Council arrangements over the induction process for new starters are not robust enough to ensure that the induction was thoroughly and completely done, i.e. the induction sheet has been signed by Staff and the Line Manager that should be sent back to Personnel. This was also raised by Internal Audit in 2007, stating that issuing the policies does not provide adequate assurance that they will be read, understood and complied with. In addition, the policies themselves do not reflect the current structures and technologies in use at the Council.</p> <p>Ineffective policy communication increases the risk of poor acceptance or understanding of security policies which may contribute to a breakdown in control and may ultimately lead to compliance and security issues.</p> <p>c We are reiterating the issue raised by the Internal Audit report in 2007, where the observation was made that it is not clear what status the policy documents have, who owns the documents, who the author/reviewer is, when the next review is</p>	<p>consider developing and implementing a more effective policy communication method that would educate all users on security and related risk.</p>		<p>contains within it a detailed Information Security Policy. This will communicated across MCC.</p>	<p>Approval will be required by the full Executive and is anticipated by June 30.</p>

Information Security Management 2009/10

Matter arising	Recommendation	Priority	Management Response	Officer Responsible and Implementation Date
<p>due or if the policy is mandatory or for guidance only.</p> <p>Without effective ownership and document control processes the policies have become out of date and are no longer effective.</p>				
<p>3 Incident Management Team Within the organisation structure of ICT, there is a Service Delivery Manager (SDM) for Incident and Problem Support who is responsible for dealing with the incidents and problems as they occur. A 'virtual' Incident and Problem management team, whereby staff from different areas of the ICT team can be pulled together to deal with incidents and problems, assists as necessary. Where incidents are critical, we believe that resource will not be a concern because of the urgency to resolve the issue.</p> <p>We understand that there are plans for a dedicated team under the Operations Manager for Maintenance and Fixes. However, this team has not yet been established.</p>	<p>We recommend that Management establishes a team for handling information security matters.</p>	<p>Medium</p>	<p>There will be a dedicated team that will focus on information security generally, including improvement projects, solution design, product evaluation and risk management. The team will not be dedicated to just information security incidents, although the management of such will form part of their remit.</p>	<p>Chief Information Officer (Steve Park)</p>

Information Security Management 2009/10

Matter arising	Recommendation	Priority	Management Response	Officer Responsible and Implementation Date
<p>4 Security Monitoring There is a security team of seven people managing the processes over patches, antivirus, firewalls and proxy, and asset management.</p> <p>Within the current structure, there is no role assigned to monitoring compliance with security policies and standards, although there are plans to establish such a role do this as part of the on-going work around the restructure of the team. There is also no established process for monitoring security. We recognise that there are plans to put in a process to have an independent third party perform planned penetration testing, as follows:</p> <ul style="list-style-type: none"> • monthly tests for external facing servers • 3 or 6 monthly tests for internal servers on a rolling basis. 	<p>We recommend ICT management push through with plans to formally establish the role of security compliance within the information security team and to provide a formal process to monitor internal and external network security via planned penetration testing exercises.</p>	<p>Medium</p>	<p>Agreed</p> <p>This role of security compliance will form part of the new IT Architecture Group, that will have within it an Information Architect. The establishment of this role will include processes to monitor networks and remediate weaknesses identified through penetration testing.</p>	<p>Chief Information Officer (Steve Park)</p> <p>June 30 2010</p>
<p>5 Formal Incident Management Process At the time of our review, there was no formally established and documented incident management and reporting process, although we recognise that informal procedures are in place, for example, an incident report as well as an action plan spreadsheet is used to capture incidents.</p> <p>We commend ICT management for initiating awareness workshops within ICT staff to promote the practice of logging incidents and</p>	<p>We recommend ICT Management establish a formal information security event reporting procedure which allows for security events to be reported to ICT as quickly as possible.</p> <p>Together with the incident reporting procedure, an incident response and escalation procedure should also be established, setting out the action to be taken on receipt of a report of an incident. Given that the original target date to</p>	<p>Medium</p>	<p>Agree</p> <p>The Microsoft network monitoring tool System Centre has been purchased and is in the process of being implemented as planned. Allied to this procurement and implementation the new Incident & Reporting Manager has undertaken to review</p>	<p>Chief Information Officer (Steve Park)</p> <p>May 31 2010</p>

Information Security Management 2009/10

Matter arising	Recommendation	Priority	Management Response	Officer Responsible and Implementation Date
<p>escalating to the Incident and Problem Service Desk Manager (SDM) as a central point of contact for incident handling and resolution. However, without an established process over incident management, there is no consistent and coordinated way to ensure that information security events and weaknesses are communicated in a manner allowing timely corrective action to be taken.</p> <p>From a sample incident walked through, we also noted that there are number of network monitoring tools, i.e. PTC, Nagios, and Solarwinds, that are utilised to identify any network or server downtimes. Various teams are assigned responsibility to monitor the alerts from these tools. However, this is not performed in coordinated manner. There is currently no interface between the network monitoring tools and the Service Desk system, HBM, aka Touchpaper, for the alerts generated in the event of any network or service failures. This increases the likelihood that incidents may not be resolved in a timely manner by the most appropriate people.</p> <p>We do recognise that Management is in the project initiation phase of acquiring Microsoft's System Center Operations Manager (SCOM), which is expected to address the issue of a</p>	<p>acquire SCOM in December 2009 has already been delayed, interim procedures need to be robust to ensure all critical alerts from existing network monitoring tools flow through to the Service Desk system for timely resolution.</p>		<p>internal procedures with advice being sought from Ernst & Young.</p>	

Information Security Management 2009/10

Matter arising	Recommendation	Priority	Management Response	Officer Responsible and Implementation Date
comprehensive network monitoring tool for the whole Council estate.				
<p>6 Network Account Security Settings There is adequate password security over network accounts. However, the settings for account lockout are not set to a maximum number of invalid attempts to login. Best practice considerations would include the following aspects:</p> <p>Account lockout duration - determines the length of time before an account is unlocked and a user can try to log on again. Account lockout threshold - determines the number of attempts that a user can make to log on to an account before it is locked. Reset lockout counter after - determines the length of time before the Account lockout threshold resets to 0 and the account is unlocked.</p> <p>Vulnerabilities can exist when these settings are not configured adequately (i.e. brute force password attacks to gain unauthorised access to network and systems/data).</p>	<p>We recommend ICT revisit security settings for account lockout and set them in line with best practices, for example, as highlighted below:</p> <ul style="list-style-type: none"> - account lockout duration - 30 minutes - account lockout threshold - 3 or more attempts - reset lockout counter after - 30 minutes 	<p>Medium</p>	<p>Agreed</p> <p>These settings will be defined in the imminent Corporate Information Security Policy and will be implemented as part of the ongoing remediation work in Active Directory.</p>	<p>Chief Information Officer (Steve Park)</p> <p>First draft April 30 2010 Approval expected June 30 2010</p>
<p>7 Issues from our previous audits Issues arising from the follow up audit in November 2009 around the following were still outstanding as at March 2010:</p> <ul style="list-style-type: none"> • No updated IT security policies (as stated in issue no. 2) 	<p>We recommend Management to develop a consolidated list of audit issues and agreed action plans to keep track of all audit commitments and to facilitate the completion of action plans as agreed. There should be regular reporting of the</p>	<p>High</p>	<p>Agreed</p> <p>Audit action plans have now been developed and are tracked through weekly ICT</p>	<p>Chief Information Officer (Steve Park)</p> <p>April 2010</p>

Information Security Management 2009/10

Matter arising	Recommendation	Priority	Management Response	Officer Responsible and Implementation Date
<ul style="list-style-type: none"> • Planned purchase of the system monitoring solution, i.e. SCOM, has been delayed. • Staff consolidation exercise and staff recruitment not completed with progress in this area slow • Network administrative privileges not restricted appropriately • User account management arrangements still to be finalised, i.e. no documented starter process, no automated leavers process, no regular review of inactive accounts • Password security still to be finalised, i.e. screensaver passwords are not set within the Active Directory • Remote access arrangements still to be finalised and signed off, i.e. the Secure Remove Access process is not consistently implemented. There is also no formal and regular process to review remote access accounts to identify accounts for deletion <p>Progress with these has not been made primarily due to competing commitments and projects.</p>	<p>action plans to keep track of the completed and ongoing activities.</p>		<p>Management Meetings.</p> <p>Progress has been made on all fronts, however, the deadlines for completion in some limited cases has slipped due to i) unforeseen events (outages) that have resulted in resource being temporarily prioritised on resolution, and ii) priority projects to support transformation (e.g. One First Street, CRM & Intranet).</p>	



www.grant-thornton.co.uk

© 2010 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