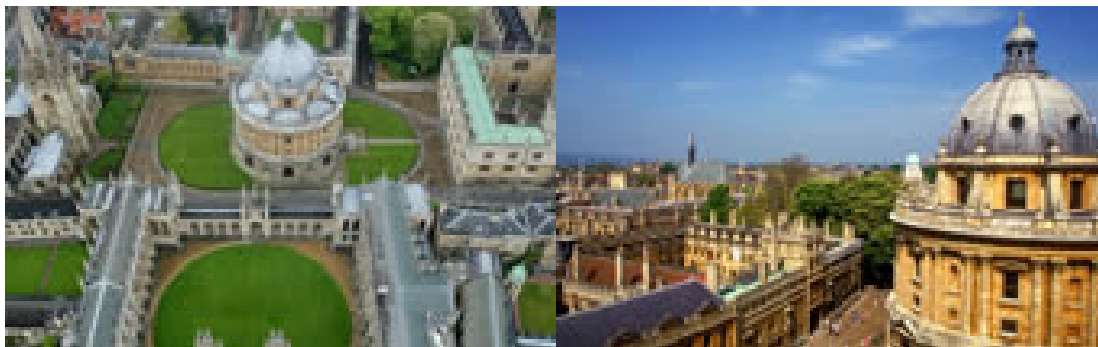


Oxford City Council

Review of ICT Security

Internal Audit Report 09/10 OP 2.3.1 Final Report



Assurance rating for this review	Moderate Assurance
---	--------------------

Distribution List
Ben Brownlee – Head of Business Transformation
David Oakes - ICT Manager
Nigel Pursey – Interim Executive Finance Director
Penny Gardner & Sarah Fogden - Head of Finance

Contents

Background and Scope.....	3
Our Opinion & Assurance Statement.....	5
Executive Summary.....	6
Limitations and Responsibilities.....	8
Findings and Recommendations.....	9
Appendix 1. Terms of Reference.....	22
Appendix 2. Assurance Ratings.....	25

Background and scope

Introduction

This review was undertaken as part of the 2009/10 Internal Audit Plan agreed by the Audit and Governance Committee.

This report has been prepared solely for Oxford City Council (the Council) in accordance with the terms and conditions set out in our letter of engagement. We do not accept or assume any liability or duty of care for any other purpose or to any other party. This report should not be disclosed to any third party, quoted or referred to without our prior written consent.

Background

Robust ICT security controls and associated management practices are fundamental to the continued, effective and efficient provision of secure services to the Council's customers, employees and partners. This review examined if the ICT security risks faced by the Council are being effectively managed and controlled.

Approach and scope

Approach

Our work is designed to comply with Government Internal Audit Standards [GIAS] and the CIPFA Code.

Scope of our work

In accordance with our Terms of Reference (Appendix 1), agreed with the Head of Business Transformation we undertook a full scope audit of ICT Security.

This audit involved a review of the ICT controls and associated management practices in place to determine whether the controls are appropriate and operating in practice.

Limitations of scope

The scope of our work was limited to those areas identified in the terms of reference.

Staff involved in this review

We would like to thank all client staff involved in this review for their co-operation and assistance.

Name of client staff

David Oakes – ICT Manager

Simon Park – ICT Service Manager

Mike Newman – Corporate Secretariat Manager

Janice Brown – Team Leader

Phil Adlard – Projects & Improvement Manager

Joanna Hargreaves – Risk Manager

Sean Hoskin – Payroll and HR Administration Manager

Victoria Fensome – Information Systems Manager

Martin Cliff – Web Projects Manager

Gerrard Barker – Oxfordshire County Council ICT Liaison Manager

Julian Shead – Oxfordshire County Council Senior Systems Engineer





Martin Taylor – Oxfordshire County Council ICT Operations Manager

Our opinion and assurance statement

Introduction

This report summarises the findings of our review of ICT Security.

Each of the issues identified has been categorised according to risk as follows:

Risk rating	Assessment rationale
 Critical	Control weakness that could have a significant impact upon, not only the system, function or process objectives but also the achievement of the authority's objectives in relation to: <ul style="list-style-type: none"> • the efficient and effective use of resources; • the safeguarding of assets; • the preparation of reliable financial and operational information; and • compliance with laws and regulations.
 High	Control weakness that has or is likely to have a significant impact upon the achievement of key system, function or process objectives. This weakness, whilst high impact for the system, function or process does not have a significant impact on the achievement of the overall authority objectives.
 Medium	Control weakness that: <ul style="list-style-type: none"> • has a low impact on the achievement of the key system, function or process objectives; and • has exposed the system, function or process to a key risk, however the likelihood of this risk occurring is low.
 Low	Control weakness that does not impact upon the achievement of key system, function or process objectives; however implementation of the recommendation would improve overall control.

Executive Summary

<p>Department: ICT Services</p> <p>Audit Owner: Ben Brownlee - Head of Business Transformation</p> <p>Date of last review: Not Applicable</p>	<p>Overall Opinion: Moderate Assurance</p> <p>The Council has made significant recent progress in implementing ICT security controls and associated management practices. Our review established that there are some weaknesses in the design and/or operation of controls which could impair the achievement of the objectives of the system, function or process. However, either their impact would be less than significant or they are unlikely to occur.</p>	<p>Scope of the Review: Robust ICT security controls and associated management practices are fundamental to the continued, effective and efficient provision of secure services to the Council's customers, employees and partners. This review examined if the ICT security risks faced by the Council are being effectively managed and controlled.</p>	<p>Key Areas of Risk considered:</p> <ul style="list-style-type: none"> • Lack of appropriate ICT Security polices and responsibilities • Inappropriate technical ICT security mechanisms and ICT security management practices • Third party and user access to Council networks and systems is appropriately controlled • ICT Risks are not managed appropriately in conjunction with Councils Third party IT outsource provider • GCSX Code of Connection non compliance 	<p>Number of Control Weaknesses identified</p> <p>0 Critical</p> <p>0 High</p> <p>10 Medium</p> <p>5 Low</p>
<p>Conclusion:</p> <ul style="list-style-type: none"> • An IT security policy is in place and responsibilities for security have been defined • A security awareness and training program is ongoing • GCSX Code of Connection compliance has been achieved and plans are in place to maintain compliance • Appropriate perimeter security mechanisms and controls are in place however intrusion detection and security monitoring could be improved • The security controls over USB keys and hand held devices could be improved • Third party IT outsource provider needs to make some improvements in security management practices to reduce the level of risk to the Council 				

Areas of Good Practice

Our review identified the following areas of good practice:

- An ICT security policy is in place and responsibilities for security have been defined
- Information Asset Owners have been defined
- A security awareness and training program is ongoing
- GCSX Code of Connection compliance has been achieved and plans are in place to maintain compliance
- Appropriate perimeter security mechanisms such as firewalls are in place
- A laptop encryption program is in place and ongoing
- Penetration testing has been performed to identify network security vulnerabilities
- An information management project is ongoing within the Council which will identify sensitive data and how it is managed
- The Council provides staff with encrypted USB keys

Limitations and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken a review of ICT Security, subject to the following limitations.

Internal control

Internal control, no matter how well designed and operated, can provide only **reasonable** and not absolute assurance regarding achievement of an organisation's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the possibility of poor judgement in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Future periods

The assessment of controls relating to ICT security is that historic evaluation of effectiveness is not relevant to future periods due to the risk that:

- the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or
- the degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

We shall endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we shall carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.

Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations or other irregularities which may exist, unless we are requested to carry out a special investigation for such activities in a particular area.

Findings and recommendations – ICT Security

Ref	Specific risk	Control weakness found	Risk rating	Recommendations	Management response	Officer responsible & implementation date
Operating Effectiveness						
1	Lack of understanding and formal compliance with the City Council security policies may lead to security administration practices being adopted by County Council staff that are not aligned with the security requirements of the City Council.	<p>Oxfordshire County Council (County Council) as part of the ICT outsource contract is expected to implement certain aspects of Oxford City Council (City Council) Security Policy.</p> <p>Interviews with County Council ICT staff established that awareness of City Council Security policy is low amongst County Council ICT Staff.</p>	<p>● Low</p>	<p>The City Council should perform a gap analysis to understand if and where the County Council security policy differs from City Council security policy to determine if this could potentially impact on the achievement of City Council ICT security requirements and objectives.</p> <p>County Council ICT staff should undertake the security policy and awareness training developed by the City Council to ensure full understanding of City Council security policy and requirements.</p>	Agreed, we will undertake the gap analysis and require County ICT staff to undertake training in the small amount of areas where our security policy differs.	<p>David Oakes, ICT Manager.</p> <p>30 April 2010</p>

Ref	Specific risk	Control weakness found	Risk rating	Recommendations	Management response	Officer responsible & implementation date
2	In the event of a catastrophic failure, the Council may not be able to recover key ICT systems and networks within an acceptable timescale resulting in business disruption.	<p>The City Council has a contract with ICM for recovery of ICT services which expires in April 2011. We understand that this has last been tested in 2008/09.</p> <p>We were informed that after the ICM contract expires; the City Council would rely upon the Disaster Recovery plan implemented by the County Council to recover its ICT systems and networks.</p> <p>The current version of the Oxfordshire County Council Disaster recovery plan which also covers Oxford City Council systems has not yet been tested.</p> <p>Additionally the agreement between the City Council and County Council does not contain formally agreed timelines for recovery of IT Systems belonging to the City Council.</p>	<p>●</p> <p>Low</p>	<p>Management should seek clarification from County Council regarding its plans to develop and test the Disaster Recovery plan and establish when it is fit for purpose.</p> <p>Once migration of data centre is completed, the disaster recovery plans should be reassessed to ensure they remain valid and up-to-date.</p> <p>IT Disaster Recovery plans should be tested on a regular basis to ensure procedures is up to date and sufficient.</p> <p>Timelines for recovery of ICT systems and services should be formally agreed as part of the agreement with the County Council.</p>	<p>Agreed – clarification has already been requested and planning for testing has begun.</p> <p>Testing will be carried out at least annually to the agreed timelines for recovery in place in the ICT contract.</p>	<p>David Oakes, ICT Manager.</p> <p>30 April 2010</p>

Ref	Specific risk	Control weakness found	Risk rating	Recommendations	Management response	Officer responsible & implementation date
3	There is a risk of unauthorised access to sensitive information and data held within the City Council Networks and Systems.	<p>We were informed that no user access reviews have been performed recently, to determine who has access to particular network shared drives and if the access rights granted are appropriate.</p> <p>Similarly no formal reviews have been performed to determine and validate the level of access available to users in the applications such as CRM and Iworld.</p>	<p>● Medium</p>	<p>The user access rights to network shares should be reviewed, to ensure that only authorised City Council staff can access the specific network shares they are entitled to access.</p> <p>Formal reviews covering user access rights within applications in the system should be performed to identify any remove any excess privileges available to users.</p>	Agreed, reports on access rights have been requested to review and amend access rights and this will be carried out regularly	Simon Park, ICT Services Manager. 30 April 2010

Ref	Specific risk	Control weakness found	Risk rating	Recommendations	Management response	Officer responsible & implementation date
4	<p>There is the risk of unauthorised access to sensitive information.</p> <p>Additionally sensitive information could be stolen resulting in data loss, negative publicity, regulatory censure and fines.</p>	<p>Former City Council IT Staff who have transferred across to the County Council are still involved in data manipulation and the handling of sensitive and confidential information.</p> <p>An example is the Benefit Fraud Team's monthly report containing highly sensitive information which is sent to the Department of Works and Pensions (DWP). A County Council employee encrypts and emails the data to the DWP.</p> <p>The City Council plans to bring in house some tasks involving sensitive data. Any third party access to sensitive data will be granted according to their contract of service which contains information confidentiality clauses.</p>	<p>●</p> <p>Medium</p>	<p>The City Council should identify all areas where County Council staff are involved in handling sensitive City Council data.</p> <p>Where possible all data manipulation and handling of sensitive data should be performed by City Council staff.</p> <p>A risk assessment should be performed of exceptions where County Council staff cannot be excluded from accessing, handling and manipulating sensitive data and appropriate compensating controls such as auditing, monitoring and logging implemented.</p> <p>Regular reporting should be implemented that identifies which County Council staff have access to sensitive City Council information.</p>	<p>Agreed, City Council has identified the tasks which require County ICT staff to handle sensitive data. As part of the project to consider transfer of appropriate duties to the relevant Service Areas, these tasks will be prioritised and brought back under the control of the City Council where possible. A risk assessment will be carried out for those activities that are to remain with the County ICT.</p>	<p>Simon Park' ICT Services Manager.</p> <p>14 May 2010</p>

Ref	Specific risk	Control weakness found	Risk rating	Recommendations	Management response	Officer responsible & implementation date
5	There is a risk of unauthorised access to Council networks, systems and services.	<p>There is a joiners and leavers process in place. However the leaver reviews which are performed on a monthly basis, do not cover temporary or contract staff.</p> <p>Reports are provided by Oxfordshire County Council on the number of active network accounts, as the City Council is charged on a per user basis. However, no user account activity reports are produced that identify network accounts that have not been accessed or used for a period of time.</p>	<p>● Medium</p>	<p>Management should ensure that the leaver reviews also cover temporary and contractual staff.</p> <p>Management should perform an audit to identify any old or redundant accounts used by temporary and contract staff that are still present on Council networks and systems.</p> <p>The City Council should liaise with County Council ICT staff to implement user account activity monitoring and reporting.</p>	<p>Agreed, temporary and contract staff will be incorporated into the Leavers procedure.</p> <p>Audit of old or redundant accounts already underway and account activity monitoring and reporting to discussed with County ICT and implemented where practicable.</p>	<p>Simon Park, ICT Services Manager.</p> <p>31 March 2010</p>

Ref	Specific risk	Control weakness found	Risk rating	Recommendations	Management response	Officer responsible & implementation date
6	There is a risk that performance against potential security lapses is not measured appropriately and discussed at the right level.	The reports received from Oxfordshire County Council over Network and Server availability and performance do not include any information over operational security such as the number of virus outbreak detected and corrected, number of hacking attempts identified.	● Low	Management should ensure that reporting against appropriate security metrics is included in the performance reports received from Oxfordshire County Council.	Agreed, ability to report against security metrics to be discussed with County ICT and included in monthly Service Reports from County ICT if possible. If not possible other reporting options to be investigated.	David Oakes, ICT Manager. 31 March 2010
7	There is a risk that unauthorised access is gained to sensitive Council data held on unencrypted storage media resulting in data loss, negative publicity, regulatory censure and fines.	Although Council supplied encrypted USB keys are made available to Council staff and USB autostart has been disabled to reduce the risk of any virus outbreaks occurring, the USB ports on desktop PCs and laptops have not been restricted to prevent the use of non encrypted USB keys or other electronic storage devices.	● Medium	The USB ports on Desktop PCs and laptops should be restricted to prevent users from copying data to non Council supplied USB keys or other electronic storage devices such as music players and SD or compact flash cards.	Agreed, the USB ports on PCs should be disabled by default and only enabled where there is a valid Business Case to do so.	David Oakes, ICT Manager. 31 May 2010

Ref	Specific risk	Control weakness found	Risk rating	Recommendations	Management response	Officer responsible & implementation date
8	Potentially leakage of sensitive information could occur if these handheld devices are lost or stolen.	<p>Council users have hand held mobile devices such as Palm Pilots and PDAs made available to them for use.</p> <p>These are currently not encrypted and are not able to be remotely disabled, measures which would render them useless if stolen.</p>	<p>● Medium</p>	<p>Management should consider adopting a two tier approach Any users who have the requirement to store sensitive or protectively marked information (personal protect, confidential, restricted) should be provided with a Blackberry device which meets Government CESG standards.</p> <p>Other users who require mobile devices for specific job requirements or who do not handle sensitive information should continue to use the devices currently in use.</p>	<p>Agreed, two tier approach as outlined to be adopted. Users of protectively marked information to be issued with Blackberrys.</p> <p>Work required to identify these users and for Services to fund.</p>	<p>Simon Park, ICT Services Manager.</p> <p>31 May 2010</p>


Ref	Specific risk	Control weakness found	Risk rating	Recommendations	Management response	Officer responsible & implementation date
9	<p>There is a risk that critical security patches are potentially missing from network equipment exposing the City Council to unauthorised access of its systems and networks.</p> <p>Additionally this may be in breach of the GCSX Code of Connection requirements.</p>	<p>Although Oxfordshire County Council regularly implements Security patches for network equipment, an audit using automated scanning tools has not been performed since June 2008.</p> <p>A list of network assets was prepared after the previous scan in 2008 and this list is updated manually. Although efforts are made to keep it up-to-date, potentially there may be critical patches missing off network equipment.</p>	<p>● Low</p>	<p>The Council should ensure that Oxfordshire County Council perform an audit to ensure that the current patch position is identified for all network equipment and any critical missing patches are applied.</p>	<p>Agreed, discussion to be had with County ICT, possibly in relation to GCSX compliance to find out whether County ICT have the facilities to perform regular automated scans for patch status of network equipment.</p> <p>If no facility currently exists to discuss with County the way forward to cover this risk.</p>	<p>David Oakes, ICT Manager.</p> <p>30 June 2010</p>

Ref	Specific risk	Control weakness found	Risk rating	Recommendations	Management response	Officer responsible & implementation date
10	There is an increased risk that any potential hacking attempts or unauthorised access may not be prevented or go undetected.	There is currently no intrusion prevention (IPS) or Intrusion detection system (IDS) in place on the Network. Limited manual monitoring is performed by County Council IT Staff.	● Medium	Management should consider implementing IPS or IDS systems on the network, to ensure that any potential intrusions or hacking attempts are prevented or identified on a timely basis.	Agreed, IDS is a requirement for v4.1 GCSX compliance. Will need to discuss with County ICT when, how and what will be implemented and if knock on cost implication for City Council.	David Oakes, ICT Manager. 31 August 2010
11	There is an increased risk of unauthorised access to sensitive network equipment.	The administrative passwords on network equipment managed by the County Council such as Cisco routers and firewalls are not changed on a regular basis.	● Low	The administrative accounts for network equipment should be changed on a regular basis.	Agreed, passwords now being changed by County ICT and regular password regime to be agreed with County ICT with regular password changes implemented.	Simon Park, ICT Services Manager. 31 August 2010

Ref	Specific risk	Control weakness found	Risk rating	Recommendations	Management response	Officer responsible & implementation date
12	<p>There is a risk that unauthorised access to City Council networks could be gained through unsecured switch ports.</p> <p>Additionally there is a risk that unauthorised devices may be installed on City Council networks.</p>	<p>The City Council Wide Area Network does not use Network Access Control (NAC) and unused ports on network switches are not disabled for example the switch at Templar's Square office.</p>	<p>● Medium</p>	<p>All unused switch ports should be disabled if not used and a process implemented to control port usage and allocation.</p> <p>Consideration should be given to implementing a NAC system in order to control devices accessing the networks.</p>	<p>Agreed, an audit needs to be carried out of all switches within the Council by County ICT, to ensure unused ports are disabled and that no unauthorised devices are attached to the network.</p> <p>NAC will be implemented if practicable.</p>	<p>Simon Park, ICT Services Manager.</p> <p>30 September 2010</p>

Ref	Specific risk	Control weakness found	Risk rating	Recommendations	Management response	Officer responsible & implementation date
13	Generic accounts significantly increase the risk of unauthorised access to Council networks, systems and data. Additionally there is no traceability and accountability of the actions that were performed in the event of issues requiring investigation.	<p>A formal process is in place to enable third party access to Council networks and systems only when required and disabling it when not in use. However, some third parties have continuous access to the network.</p> <p>A number of third parties access Council networks and systems using generic accounts.</p>	<p>● Medium</p>	A review should be performed to identify all third party generic accounts. These parties should be given accounts that can identify individual users who access using these accounts.	Agreed, an audit of all third party access, the access method used, the regularity and systems they need access to needs to be carried out and kept up to date by County ICT.	<p>Simon Park ICT Service Manager.</p> <p>29 October 2010</p>

Ref	Specific risk	Control weakness found	Risk rating	Recommendations	Management response	Officer responsible & implementation date
14	There is an increased risk of critical security issues not being responded to appropriately and in a timely manner.	<p>Although a process is in place for notification of incidents by text and email to the City Council, there is no formal criteria established describing what level of incidents should be notified to the City Council together with timescales for notification.</p> <p>There have been some instances of security incidents not being reported to City Council staff.</p> <p>An example of such incident is a network outage early on 17th August 2009 when a significant portion of the City Council Data Network was down. City Council Management were not made aware until mid morning.</p>	<p>● Medium</p>	The Council should establish formal criteria in terms of what security incidents are reported on by Oxfordshire County Council together with the timescales for reporting.	City Council already in consultation with County ICT to rectify these notification issues. Process being developed and controls being agreed.	<p>Simon Park, ICT Services Manager.</p> <p>30 April 2010</p>

Ref	Specific risk	Control weakness found	Risk rating	Recommendations	Management response	Officer responsible & implementation date
15	There is a risk that sensitive data may be left on pool laptops which is then accessed by unauthorised users.	We were informed that pool laptops are available to Council staff for use and these laptops are encrypted with the SafeBoot product. However, the procedure for removing any potentially sensitive data left on these laptops by users is currently not formalised and sometimes does not take place.	 Medium	Management should formalise the procedure for removing data from pool laptops before reuse.	Agreed, procedure to be agreed, documented and implemented.	David Oakes, ICT Manager. 29 October 2010

Appendix 1 - Terms of Reference

Objectives and deliverables

Objectives

Robust ICT security controls and associated management practices are fundamental to the continued, effective and efficient provision of secure services to the Council's customers, employees and partners. This review will examine if the ICT security risks faced by the Council are being effectively managed and controlled.

Deliverables

Our deliverable will be a report detailing our findings with regard to our assessment of the level of control in place regarding ICT security and the level of assurance we can place on the control environment

Listed below is the information that may be required at the commencement of the audit:

- IT Security policies;
- Operational ICT security management documentation;
- Any internal security reviews undertaken such as a Data Handling Assessment;
- Code of Connection compliance statement;
- Network diagrams of internal networks and external connectivity;
- Results of any penetration testing or scanning.

The list is not intended to be exhaustive. Evidence should be available to support all operating controls. Other information arising from our review of the above documentation may be requested on an ad hoc basis.

Scope and approach

Our work will focus on identifying the guidance, procedures and controls in place to mitigate key risks through:

- Documenting the underlying guidance, policy and processes in place and identifying key controls;
- Considering whether the ICT security management practices, policies and procedures in place are fit for purpose; and
- Testing key controls.

The review will require the following input from Oxford City Council and delivery partners:

- Two ½ day sessions with Oxfordshire County Council ICT staff responsible for Oxford City Council ICT Security;
- 10 one hour interview sessions with Oxford City Council staff including Service representatives. Other interview sessions may be required as the review progresses;
- Interviews and documents will be requested two weeks in advance where possible.

The key points that we will focus on are:

- Establish that ICT security policies are in place;
- Identify the responsibilities for ICT security within the Council (structure, policy and delivery);
- Review the technical ICT security mechanisms (both at the perimeter and internally) in place that protect key systems, sensitive information and assets;
- Review the ICT security management practices in place such as monitoring, incident management and reporting;
- Establish that external third party and user access to Council networks and systems is appropriately controlled;
- Examine how ICT Security risks are managed in conjunction with the Council's third party IT outsource provider;
- Examine the Council's existing GCSX Code of Connection compliance statement;
- Determine how the Council will maintain ongoing GCSX compliance.

We will discuss our findings with the Head of Business Transformation or nominated representative to develop recommendations and action plans. A draft report will be issued to all relevant officers for review and to document management responses.

Limitation of Scope

The scope of our work will be limited to those areas identified in the terms of reference. We will not perform detailed reviews of IT equipment configuration, system or application configurations.

Stakeholders and responsibilities

Head of Business Transformation	Ben Brownlee	<ul style="list-style-type: none"> ▪ Review draft terms of reference ▪ Review and meet to discuss issues arising and develop management responses and action plan
ICT Manager	David Oakes	<ul style="list-style-type: none"> ▪ Review draft report. ▪ Implement agreed recommendations and ensure ongoing compliance
Interim Executive Finance Director	Nigel Pursey	<ul style="list-style-type: none"> ▪ Receive agreed terms of reference ▪ Receive draft and final reports
Head of Finance	Penny Gardner / Sarah Fogden	<ul style="list-style-type: none"> ▪ Receive agreed terms of reference ▪ Receive draft and final reports
Chief Executive	Peter Sloman	<ul style="list-style-type: none"> ▪ Receive final report

Our Team and Timetables

Our team

Chief Internal Auditor	Chris Dickens
Audit Manager	Neil Ward
Auditors	Neil Ward and Saqib Iqbal

Timetable

Steps	Date
TOR approval	October 2009
Fieldwork commencement	November 2009 (T)
Fieldwork completed	T + 7 days
Draft report of findings issued	T + 3 weeks
Receipt of Management response	T + 5 weeks
Final report of findings issued	T + 6 weeks

Budget

Our budget for this assignment is 7 days. If the number of days required to perform this review increases above the number of days budgeted, we will bring this to management attention.

Terms of Reference Approval

These Terms of Reference have been reviewed and approved:

.....

Ben Brownlee
 Signature (Head of Business Transformation)



Chris Dickens
 Signature (Chief Internal Auditor)

Appendix 2 - Assurance ratings

Level of assurance	Description
High	<p>No control weaknesses were identified; or</p> <p>Our work found some low impact control weaknesses which, if addressed would improve overall control. However, these weaknesses do not affect key controls and are unlikely to impair the achievement of the objectives of the system. Therefore we can conclude that the key controls have been adequately designed and are operating effectively to deliver the objectives of the system, function or process.</p>
Moderate	<p>There are some weaknesses in the design and/or operation of controls which could impair the achievement of the objectives of the system, function or process. However, either their impact would be less than significant or they are unlikely to occur.</p>
Limited	<p>There are some weaknesses in the design and / or operation of controls which could have a significant impact on the achievement of key system, function or process objectives but should not have a significant impact on the achievement of organisational objectives. However, there are discrete elements of the key system, function or process where we have not identified any significant weaknesses in the design and / or operation of controls which could impair the achievement of the objectives of the system, function or process. We are therefore able to give limited assurance over certain discrete aspects of the system, function or process.</p>
No	<p>There are weaknesses in the design and/or operation of controls which [in aggregate] could have a significant impact on the achievement of key system, function or process objectives and may put at risk the achievement of organisation objectives.</p>

In the event that, pursuant to a request which Oxford City Council has received under the Freedom of Information Act 2000, it is required to disclose any information contained in this report, it will notify PricewaterhouseCoopers (PwC) promptly and consult with PwC prior to disclosing such report. Oxford City Council agrees to pay due regard to any representations which PwC may make in connection with such disclosure and Oxford City Council shall apply any relevant exemptions which may exist under the Act to such report. If, following consultation with PwC, Oxford City Council discloses this report or any part thereof, it shall ensure that any disclaimer which PwC has included or may subsequently wish to include in the information is reproduced in full in any copies disclosed.

©2010 PricewaterhouseCoopers LLP. All rights reserved. 'PricewaterhouseCoopers' refers to PricewaterhouseCoopers LLP (a limited liability partnership in the United Kingdom) or, as the context requires, other member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.