INFRASTRUCTURE, GOVERNMENT AND HEALTHCARE

Internal Audit Service 2008/09 Progress report (3)

Oxford City Council

25th November 2008

AUDIT

AUDIT ▪ TAX ▪ ADVISORY

Contents

This report is provided pursuant to the terms of the contract with Oxford City Council. The report is intended solely for internal purposes by the management and Members of Oxford City Council and should not be used by or distributed to others, under the Freedom of Information Act 2000 or otherwise, without our prior written consent. To the fullest extent permitted by law, KPMG LLP does not assume any responsibility and will not accept any liability in respect of this Report to any party other than the Beneficiaries.

Audit Plan / Timing 2008/09

	Area	Planned Days	Timing	Scope
Authority Wide				
1	**Corporate Governance**	10	January 2009	Further enhancements are required within this area to improve the use of resources score received. We will focus on a couple of key issues to aid in the development of this area.
2	**Risk management**	15	Completed with on – going support	We have assisted the Authority in the development of a revised risk register format, attended a Wider Leadership Team to promote risk management, established a Risk Group to champion risk management, and given a training session to Members on risk management. We also assisted in the development of the 2007/08 year end risk register, meeting with Heads of Service to populate the register.
3	**Equality and Diversity**	15	November 2008, to be completed after first impact assessments have been completed.	This area has not been subject to a review by internal audit (brought forward from 2007/08). We will review the overall arrangement for ensuring equality and diversity across the organisation against good practice.
4	**Health and Safety follow-up**	6	December 2008, to be completed after milestone dates for recommendations have been reached.	This area was assessed as weak at the review in 2006/07, and follow up in 2007/08 identified recommendations remained outstanding. Members require independent assurance that controls and procedures are operating as intended and as such we will continue to review progress in the implementation of agreed actions.
5	**Single status**	6	To be completed prior to full costed proposal milestone of January 2009.	This review was requested by management and involves a validation of the single status pay model base data.
6	**Business Continuity/** **Disaster Recovery**	10	Final report issued 7 November 2008 WEAK	The Authority has been reviewing its arrangements in light of recent issues, including the Oxford floods in 2007. We have reviewed the progress made by the Authority in implementing its action plan.

Audit Plan / Timing 2008/09

	Area	Planned Days	Timing	Scope
Finance and Asset Management				
7	**Benefits**	15	December 2008	Managed audit – essential for DA reliance. Satisfactory ratings in 2005/06 and 2006/7 and good in 2007/08. We propose a similar compliance type audit due to the significance and value of the transactions.
8	**Local Taxation**	10	December 2008	Managed audit – essential for DA reliance. Satisfactory ratings in 2005/06 and good / satisfactory ratings in 2006/07 progressing to good in 2007/08. We propose walkthrough testing for both NNDR and Council tax.
9	**Payroll**	10	December 2008	Managed audit – essential for DA reliance. Satisfactory ratings in 2005/06 to 2007/08. We propose to undertake compliance testing.
10	**Accounts payable**	5	January 2009	Managed audit – essential for DA reliance. Satisfactory ratings to in 2005/6 and 2006/7 and good in 2007/08. We propose to carry out walkthrough testing.
11	**Accounts receivable**	5		Managed audit – essential for DA reliance. Satisfactory ratings to in 2005/6 and 2006/7 and good in 2007/08. We propose to carry out walkthrough testing.
12	**Main accounting**	5		Managed audit – essential for DA reliance. Satisfactory rating to date. We propose to undertake walkthrough testing to confirm that the design of the controls has not changed.
13	**Treasury management**	5		Managed audit – essential for DA reliance. Good rating to date. We propose to undertake walkthrough testing to conform that the design of the controls has not changed.
14	**Fixed Assets**	10	December 2008	Managed audit – essential for DA reliance. We propose to undertake compliance testing in this area.

Audit Plan / Timing 2008/09

	Area	Planned Days	Timing	Scope
Business Systems				
15	**Data Security**	10	Final report issued 7 November 2008 WEAK	We have reviewed the arrangements the Authority has in place which ensures the safe keeping of information both on and off site.
City Regeneration				
16	**Building Control / Planning / Inspection/ Enforcement**	20	January 2009	We will review the controls in place over application processing, inspection and enforcement which ensure compliance with documented procedures.
17	**Taxi Licensing**	15	Final report issued 10 September 2008 WEAK	We have reviewed the controls in place over the approval and review of taxi licences which ensure compliance with documented procedures.
City Services				
18	**Local Financial Systems**	15	October/November 2008 Work completed early November. Draft report being prepared.	We have reviewed the local systems for receipting and collecting income within trade waste, leisure and the tourist information centre. We have also followed up the implementation of recommendations made in relation to the parks cash collection which was graded as weak in 2007/08.
19	**Housing Repairs**	20	October/November 2008 Work completed mid November . Draft report being prepared.	We have completed an end to end review of the responsive repairs process, from initial enquiry through to post inspection. We have also reviewed the controls in place for recharging tenants for repairs which are their responsibility.
20	**Leaseholder recharging**	10	January 2009	We propose to review the processes in place which ensure compliance with legislation with the recovery of all income due to the Authority, including the approval of write-offs of bad debt.
21	**Car Parking**	10	Final report issued 10 September 2008 WEAK	We have reviewed the overall arrangements in respect of car parking including the implementation of the car parking strategy, setting and collecting of charges, and compliance with legal obligations.

Audit Plan / Timing 2008/09

	Area	Planned Days	Timing	Scope
VFM				
22	**VFM follow up**	10	Work has commenced on three of the four reviews. To report January Committee	Members need assurance that management are beginning to implement the outcomes of value for money reports that have been agreed by the Audit & Governance Committee. We propose to undertake follow-up work on the Capital Programme, Street Cleaning, Vehicle Maintenance and Housing Repairs.
23	**Leisure Market Testing**	20	Work commenced. To report progress to January Committee.	The market testing of Leisure Services is a major project for the City Council and is very important in delivering the savings required for 2009/10 and beyond. Members were keen that KPMG should have a role reviewing the project as it unfolds, rather than waiting until the end of the process. We will use our experience of market testing to discuss alternative approaches with relevant officers/Members and will keep the Audit & Governance Committee informed of progress.
24	**VFM Mapping**	7	Completed	This exercise commenced in 2007/08 and is attempting to collate all the available empirical evidence of the comparative cost and quality of individual services and will enable the Authority to make better informed decisions on the areas it should prioritise for improved VFM.
25	**VFM studies**	13	To be identified	As with last year, we have allowed some VFM days to be commissioned on a "call-off" basis by the Audit & Governance Committee and officers in order to address emerging issues.
Contingency				
26	**Contingency**	25		15 days utilised in relation to grant claim audits. 5 days utilised for further risk management support.

KPMG

INFRASTRUCTURE, GOVERNMENT AND HEALTHCARE

Review of Business Continuity Planning 2008/09

Overall system rating:	
▦	Weak

Oxford City Council

7 November 2008

Report status	
Date of Debrief	6 September 2008
Discussion draft issued	19 September 2008
Management responses received	6 November 2008
Final report issued	7 November 2008
Presented to Audit and Governance Committee	25 November 2008

Distribution for action	Distribution for information
Mike Newman, Corporate Secretariat	Penny Gardner/Sarah Fogden, Head of Service – Finance Daniel Hennessy, Business Systems Manager

AUDIT ▪ TAX ▪ ADVISORY

Executive Summary

Conclusion

As internal auditors of the Authority, we provide an annual overview of the system of internal control. In arriving at this overview, we give a conclusion on the individual systems reviewed during the year. Our conclusion is either that the system is good, satisfactory, weak or unacceptable. However, in giving our conclusion, it should be acknowledged that our work is designed to enable us to form an opinion on the quality of the systems examined, based on the work undertaken during our current review. It should not be relied upon to disclose all weaknesses that may exist and therefore the conclusion is not a guarantee that all aspects of the systems reviewed are adequate and effective.

From the work performed on Business Continuity Planning, we consider there is considerable risk that the business continuity processes (or individual Business Continuity Plans) will fail to meet their objectives. Significant improvements are required to ensure the arrangements are in-line with Section 11 of the Manual of Protective Security (MoPS), BS25999 and established best practice. In particular risk assessments, maintenance and testing of business continuity plans, and the overall governance of business continuity processes need to be improved. As a result, we have graded this area as weak.

We have made four recommendations which will address the identified weaknesses. The implementation of our recommendations should enhance business continuity arrangements and provide an increased level of assurance to the Authority from the date of implementation.

Context

The audit of the Business Continuity Planning has been a identified as part of the internal audit plan for 2008/09 approved by the Audit and Governance Committee. The objectives of our review, as outlined in the terms of reference were to assess the effectiveness of the Business Continuity Plans including the management and planning processes. Effective business continuity management is a responsibility for all public sector bodies and Critical National Infrastructure organisations. Section 11 of the Manual of Protective Security (MoPS) provides guidance to assist public sector bodies in discharging their business continuity responsibilities and conforms with the recognised British Standard BS25999. We have assessed the Authority against MoPS as this covers both public sector and government best practice.

The objectives of Business Continuity Management is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters. A business continuity management process should be implemented to reduce the disruption caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventative and recovery controls. The consequences of disasters, security failures and loss of service should be analysed. Business Continuity Plans (BCPs) should be developed and implemented to ensure that business processes can be restored within the required time-scales. Such plans should be maintained and tested and be an integral part of management processes. Business continuity management should include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.

In 2006, the Authority started a process of business continuity planning which lead to the production of an Authority wide recovery plan with subsequent individual business unit business continuity plans being developed. Since the plans were developed, the Authority has undergone an internal reorganisation, which has resulted in a number of the plans becoming out of date.

During our review we were provided with information for a number of areas covering business continuity plans for Business Services, Customer Services, Environmental Health, Oxford City Homes and Human Resources. We also reviewed the Authority's overall Business Continuity Plan plus supporting documents listed at Appendix C.

Acknowledgement

We would like to take this opportunity to thank all the staff we held discussions with for their assistance and co-operation during the review.

1. Executive summary (cont'd)

This section of the report highlights the main findings of our review. Our assessment against the MoPS can be found from page 10 within the 'detailed finding' section. An action plan of recommendations is documented in Appendix A.

Business Continuity		
Objective	**Areas of good practice**	**Areas for further development**
Business Continuity Planning	Our review identified the following areas of good practice in respect of the Authority's Business Continuity Arrangements: ✓ A Business Impact Assessment (BIA) has been carried out based on one serious incident scenario and critical systems have been identified; ✓ A Authority wide Business Recovery Plan has been produced as a result of the BIA; ✓ Business Units have produced individual business continuity plans; ✓ The IT Disaster Recovery Plan has been regularly tested and test reports produced.	Our work has also identified the following areas where controls could be further strengthened: ▪ Formal arrangements should be established to provide an overall governance framework, with the Corporate Secretariat managing the business continuity process and provide governance/procedures for the format/testing and updating of plans; ▪ The Business Recovery Plan should be updated to include guidance on producing BCP, training, testing, reviewing and updating the plans and include a timetable for tests and reviews. In addition, the individual business unit business continuity plans should be kept up to date and at least one hard copy held on site with another copy at the recovery site; ▪ All the individual business unit business continuity plans should be tested annually with a full rehearsal of the Authority's Business Recovery Plan every two years; and ▪ The BIA should be revisited to identify specific events that could impact on the critical business processes. These events can then be used to assist business units in carrying out their own risk assessment when reviewing their individual plans.

The table below details the number of recommendations made, the priority assigned and those accepted by management.

Recommendations	Priority One	Priority Two	Priority Three	Total
Made	3	1	0	4
Accepted	3	1	0	4

2. Detailed Findings

Section 11 of the Manual of Protective Security (MoPS) outlines the requirements to enable public sector bodies to discharge their responsibility for implementing effective business continuity. During our assessment we compared the Council processes for business continuity against these requirement. The table below list the requirement, provides the MoPS description and our findings. The recommendations as a result of our findings are detailed in the action plan in Appendix A.

Section 11 Requirement	MoPS Description	Finding
Business continuity management	Responsibility for co-ordinating the business continuity management process should be assigned at an appropriate level within the organisation, e.g. an Information Security Forum.	There is no formally assigned ownership of the Business Recovery Plan. There was no obvious owner of business continuity management within Corporate Secretariat. At our initial meeting with the Secretariat Manager, he was not aware of a Business Recovery Plan. Only during a meeting with a former project manager, who has since changed roles, was an electronic copy of the Business Recovery Plan provided, however, this was not signed. The Authority has no information security related forums or other bodies that provide governance of business continuity issues.
Business continuity process	There should be a managed process in place for developing and maintaining business continuity throughout the organisation. It should bring together the following key elements of business continuity management: a. understanding the risks the organisation is facing in terms of their likelihood and their impact, including an identification and prioritisation of critical business processes; b. understanding the impact which interruptions are likely to have on the business (it is important that solutions are found that will handle smaller incidents, as well as serious incidents that could threaten the viability of the organisation); c. formulating and documenting a business continuity strategy consistent with the agreed business objectives and priorities; e. formulating and documenting business continuity plans in line with the agreed strategy;	There is no evidence of any process or documented procedure for developing, maintaining and updating business continuity plans within the Authority. A Business Recovery Plan has been produced for the Authority based on a Business Impact Assessment. Individual units have produced their own business continuity plans. A number of staff were aware of requirement for updating plans. However, inconsistency in updating was identified across business units. Although a Business Impact Assessment was carried out Authority wide, a sample of specific risk events, duration and probability were not identified. A single generic serious incident scenario was used to identify the impact and the related critical business systems for the Authority wide plan. There were no scenarios included in the individual business unit business continuity plans, and no anecdotal or documented evidence of business units conducting individual risk assessments.

2. Detailed Findings (cont'd)

Section 11 Requirement	Description	Finding
Business continuity process **(cont'd)**	f. regular testing and updating of the plans and processes; and g. ensuring that the management of business continuity is incorporated in the organisation's processes and structure.	The inclusion of scenarios would identify potential smaller incidents and mitigating solutions, such as regular inspection of the water tank above the server room or a fire suppression system installed in the St Aldate's building. The business unit business continuity plans are standardised and are consistent with the lay out of the Business Recovery Plan. Apart from the IT Disaster Recovery Plan within Business Services, there is no anecdotal or documented evidence that any of the plans have been tested.
Business continuity and impact analysis	Business continuity should begin by identifying events that can cause interruptions to business processes, e.g. equipment failure, flood and fire. This should be followed by a risk assessment to determine the impact of those interruptions (both in terms of damage scale and recovery period). Both of these activities should be carried out with full involvement from owners of business resources and processes. This assessment considers all business processes, and is not limited to the information processing facilities. Depending on the results of the risk assessment, a strategy plan should be developed to determine the overall approach to business continuity. Once this plan has been created, it should be endorsed by management.	A Business Impact Assessment (BIA) was carried out based on a generic serious incident scenario which closes the centre of Oxford denying access to the three council office sites. A Business Recovery Plan was produced based on the BIA. Apart from the loss of the Cowley Road site, no consideration has been given to events affecting individual business unit such as a breach of the water tank above the server room or the total loss of the St Aldgate's building to fire. These such events should be included in the business continuity framework.
Business continuity planning framework	A single framework of business continuity plans should be maintained to ensure that all plans are consistent and to identify priorities for testing and maintenance. Each business continuity plan should specify clearly the conditions for its activation, as well as the individuals responsible for executing each component of the plan. When new requirements are identified, established emergency procedures, e.g. evacuation plans or any existing fallback arrangements, should be amended as appropriate. A business continuity planning framework should consider the following:	There is no documented framework for the business continuity plans that provides any form of guidance on producing maintaining and testing the plans. The Business Recovery Strategy does not provide any guidance on risk assessment, writing business continuity plans, training, testing or reviewing the plans.

2. Detailed Findings (cont'd)

Section 11 Requirement	Description	Finding
Business continuity planning framework **(cont'd)**	a. the conditions for activating the plans which describe the process to be followed (how to assess the situation, who is to be involved, etc.) before each plan is activated; b. emergency procedures which describe the actions to be taken following an incident which jeopardises business operations and/or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities, e.g. police, fire service; c. fallback procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations, and to bring business processes back into operation in the required time-scales; d. resumption procedures which describe the actions to be taken to return to normal business operations; e. a maintenance schedule which specifies how and when the plan will be tested, and the process for maintaining the plan; f. awareness and education activities which are designed to create understanding of the business continuity processes and ensure that the processes continue to be effective; g. the responsibilities of the individuals, describing who is responsible for executing each component of the plan. Alternatives should be nominated as required. Each plan should have a specific owner. Emergency procedures, manual fallback plans and resumption plans should be within the responsibility of the owners of the appropriate business resources or processes involved. Fallback arrangements for alternative technical services, such as information processing and communications facilities, should usually be the responsibility of the service providers.	Although all the plans include specific conditions for activation, there was no reference to the anticipated duration of an incident as an activation trigger, such as if Oxford centre is to be closed for 48 hours, is it reasonable to activate the DR plan which takes 48 hours to implement. The business continuity plans audited included emergency procedures for staff but did not include sections on public relations or other public sector liaison. The business continuity plans reviewed included clear fallback procedures. The business continuity plans reviewed did not include resumption procedures. There is no documented maintenance schedule or testing programme, although some business units were aware of a requirement to update their plans every six months. There has not been any formal education and awareness activities since the initial Business Impact Assessment. However, the Environmental Health Department had recently held a BCP management workshop. All the plans reviewed had allocated owners and most had nominated individual responsibilities for executing the plan, however, some of the individuals named had left the council. The plans which were out of date were Human Resources and Customer Services, both of which had recently undergone reorganisations with a number of management changes.

2. Detailed Findings (cont'd)

Section 11 Requirement	Description	Finding
Writing and implementing continuity plans	Plans should be developed to maintain or restore business operations in the required time scales following interruption to, or failure of, critical business processes. The business continuity planning process should consider the following: a. identification and agreement of all responsibilities and emergency procedures; b. implementation of emergency procedures to allow recovery and restoration in required time-scales. c. documentation of agreed procedures and processes; d. appropriate education of staff in the agreed emergency procedures and processes including crisis management; e. testing and updating of the plans.	The plans reviewed contained the critical processes and documented procedures to be implemented to recover those processes including relocation of staff and critical systems. None of the plans reviewed documented the process of educating/training of staff in the emergency procedures. None of plans audited documented any testing programme or procedure for reviewing or updating the plans. The Environmental Health Department and Oxford City Homes had a management process for updating the plan, although this was not formally documented.
Testing the plans	Business continuity plans may fail on being tested, often because of incorrect assumptions, oversights, or changes in equipment or personnel. They should therefore be tested regularly to ensure that they are up to date and effective. Such tests should also ensure that all members of the recovery team and other relevant staff are aware of the plans. The test schedule for business continuity plan should indicate how and when each element of the plan should be tested. It is recommended to test the individual components of the plan frequently. A variety of techniques should be used in order to provide assurance that the plan will operate in real life. These should include: a. table-top testing of various scenarios (discussing the business recovery arrangements using example interruptions); b. simulations (particularly for training people in their post-incident/crisis management roles); c. technical recovery testing (ensuring information systems can be restored effectively); d. testing recovery at an alternative site (running business processes in parallel with recovery operations away from the main site);	There was no corporate guidance made available on testing either the individual business unit business continuity plans, or the Authority Business Recovery Plan. None of the business continuity plans reviewed had undergone any form of testing. The IT Disaster Recovery Plan has been regularly tested, and test reports were made available. The technical recovery of the IT Systems has been tested as well as well as the recovery of the IT system at the Cowley Road as the alternative site. There was no requirement in any of the plans reviewed to test supplier's facilities or services. We noted the BIA identified a key dependency on the provision of telephone services from Anite. There has not been any full rehearsals of the business recovery plan at a business unit or Authority wide level.

2. Detailed Findings (cont'd)

Section 11 Requirement	Description	Finding
Testing the plans **(cont'd)**	e. tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment); f. complete rehearsals (testing that the organisation, personnel, equipment, facilities and processes can cope with interruptions). The techniques can be used by any organisation and should reflect the nature of the specific recovery plan.	
Maintaining and re-assessing the plans	Business continuity plans should be maintained by regular reviews and updates to ensure their continuing effectiveness. Procedures should be included within the organisation's change management programme to ensure that business continuity matters are appropriately addressed. Responsibility should be assigned for regular reviews of each business continuity plan; the identification of changes in business arrangements not yet reflected in the business continuity plans should be followed by an appropriate update of the plan. This formal change control process should ensure that the updated plans are distributed and reinforced by regular reviews of the complete plan. Examples of situations that might necessitate updating plans include the acquisition of new equipment, or upgrading of operational systems and changes in: a. personnel; b. addresses or telephone numbers; c. business strategy; d. location, facilities and resources; e. legislation; f. contractors, suppliers and key customers; g. processes, new, changed or withdrawn; h. risk (operational and financial).	There are no documented procedures for reviewing and maintaining the plans. Although some plan owners where aware of a requirement to update the plans every 6 months, none of the plans reviewed nominated responsibility for reviewing the plans or contained a timetable for a review. The level of accuracy of the plans reviewed varied dependant on the business unit details of each business unit are at Appendix B. The plans reviewed had been updated to reflect the following: a. personnel; b. addresses or telephone numbers; f. contractors, suppliers and key customers; but not: c. business strategy; d. location, facilities and resources; e. legislation; g. processes, or h. risk (operational and financial). None of plans reviewed had been reviewed based on identification of new risks or changes to the risk assessment.

Appendix A: Recommendations

This Appendix summarises in the form of recommendations the issues arising from this review which we believe require action.

#	Priority	Issue	Risk	Recommendation	Management Response
		Governance			
1	●One	There is no formally assigned ownership of the Business Recovery Plan, and there is no evidence of any process or documented procedure for developing and maintaining business continuity within the Authority. In addition, we were also unable to identify effective training mechanisms required to ensure the effective co-ordination of business continuity processes throughout the Authority and within individual Business Units. The Authority has not developed an information security related forum or other body that could provide a governance framework for business continuity issues. Considerable effort had been required to conduct the initial BIA and produce the Business Recovery Strategy and BCPs. However, many of plans were not up to date and these may in danger of becoming obsolete.	Business Continuity Plans may be ineffective.	Corporate Secretariat should have increased involvement in Council wide business continuity processes, and should provide the governance over testing, reviewing and updating of the business continuity plans. This should include production of procedures and ensuring an effective training and awareness programme is in place. The business units should be responsible for the production, testing and maintenance of their own plans. However, there needs to guidance on how and when this should be carried out.	The Corporate Secretariat Manager will take immediate responsibility for the governance of the Council-wide business continuity plan process, to include testing, reviewing and updating of the individual business continuity plans. As an initial step, following the management restructure, individual plan owners will be identified by the Corporate Secretariat Manager for business continuity plans for each of the new 12 service areas (to be completed by end of November 2008). The Corporate Secretariat Manager will draft a procedure note by end of November 2008 on the updating of the plans, to include a training and awareness programme, based on the systems put in place in 2006. The procedure note will be amended (by end of March 2009) to take account of any changes made because of the reviews of the overall plan and the individual plans. A training and awareness programme will be identified (based on the work originally undertaken in 2006) and the findings contained in this audit report (to be completed by end of December 2008). Corporate Secretariat Manager

Appendix A: Recommendations (cont'd)

#	Priority	Issue	Risk	Recommendation	Management Response
2	●One	**Maintenance of the plans** We were provided with two versions of the individual business unit business continuity plans by Corporate Secretariat and the business continuity Project Manager. There were key differences such as emergency contact details within the plans, and configuration control was not clear. A review of the business unit plans identified that two business units did not have hard copy versions of their business continuity plans available, and the electronic copies provided were incomplete and out of date. Only one business unit confirmed they had a hard copy at the recovery location. Further details of our testing is documented in Appendix B.	Should an incident occur there is a risk that the plans will not be available to be implemented and restoration of the service may not be timely.	Corporate Secretariat should own the Authority Business Recovery Plan and ensure electronic copies of all plans are held centrally with appropriate configuration control. Arrangements should be made for the corporate review of business units plans to ensure that they are up to date. A minimum of two hard copies of each plan, should be retained, one in the business unit and one at the recovery location.	The authority Business Recovery Plan will be updated by the end of December 2008. The Corporate Secretariat Manager will review the existing plans with the identified plan owners to ensure that they are up to date and take account of the management structure changes, changes in business arrangements not identified in the existing plans, a review of risks associated with those businesses, and any other issues that might impact on the effectiveness of the plan. (Review to commence beginning December 2008; to be completed by end of February 2009). The Corporate Secretariat Manager will maintain electronic copies of the overall and individual plans. As a first step, the Corporate Secretariat Manager will immediately obtain electronic copies of the existing plans. Updated hard copies of the individual business continuity plans will be retained in each service area and at the recovery location. A hard copy of the updated overall plan will be retained at the recovery location. (To be completed following the plans' review, end of February 2009). In the meantime, a hard copy of each of the existing individual business continuity plans will be placed at the recovery location.

Appendix A: Recommendations (cont'd)

#	Priority	Issue	Risk	Recommendation	Management Response
3	●One	**Testing** Although the IT Disaster Recovery plan had been tested, there was no evidence of any testing of the individual business unit plans, and staff interviewed were not aware of any requirement or reason to test the plans. There was no requirement in any of the plans reviewed to test supplier's facilities or services.	Although the strategy and plans have been produced, without testing they may be ineffective or incomplete and restoration of the service may not be timely.	Individual business continuity plans should be tested every 12 months to confirm they are effective, identify any gaps, and produce an action plan for future improvements. Corporate Secretariat should produce an annual testing plan for all plans and obtain confirmation of test and outcomes. Testing should also cover supplier's facilities or services where significant reliance is placed on their operation.	Once the initial review of the existing individual plans has been completed, a decision will be taken whether to conduct a test based on one or more of the existing plans, to identify gaps and help inform the review/updating process), or whether instead to undertake the test after the detailed reviews have been completed. If the former is adopted, it is proposed that the test should take place in January 2009. It may be appropriate for test to carried out on one service with the results being used to help the other service areas review their plan. If the initial test is to wait until the reviews have been completed, the aim is to carry it out in June/July 2009. The Corporate Secretariat Manager will produce an annual testing programme to take place in either September (if the initial test takes place in January 2009) or in June/July (if the first test is to be carried out in June/July 2009). The testing procedure will include provision for the Corporate Secretariat Manager to receive confirmation of the tests and the outcomes.

Appendix A: Recommendations (cont'd)

#	Priority	Issue	Risk	Recommendation	Management Response
4	● Two	**Risk Assessment** The Business Impact Assessment should identify the Authorities critical processes, systems and personnel. The BIA should then identify the risk to those process, the impact and probability. These are used to produce mitigation strategies, produce the business plans and support and investment case. The initial Business Impact Assess only considered a single generic serious incident. There was no consideration of other events such as flooding of the server room or the total loss of the St Aldate's Headquarters. Business units have not conducted their own risk assessments. We also noted that Business Unit Plans did not contain: ▪business strategy; •location, facilities and resources; •legislation; •processes, or •risk (operational and financial).	There is currently no assurance that all appropriate risks or scenarios have been addressed.	We recommend that the BIA is revisited, and more realistic incidents or a selection of incidents identified together with an assessment of the impact and probability. Business Units should also conduct their own risk assessments. The Business Recovery Strategy and business continuity plans should then be reassessed against these incidents, and updated.	The Business Impact Assessment will be reviewed by the end of December 2008 to include a wider selection of possible incidents (to be included as part of the overall and individual plans review process). The review of the individual plans will include the provision of risk assessments. Corporate Secretariat Manager

Appendix B - Assessment of Business Unit BCP’s

We assessed individual business unit business continuity plans to determine whether the plans were complete, available in electronic and hard copy, had been tested and updated. The results of these assessments are shown below:

Requirement	Business Services	Customer Services	Environmental Health	Oxford City Homes	HR
BCP - Complete	√	×	√	√	×
- Electronic	√	√	√	√	√
- Hardcopy	√	×	√	√	×
- Copy held off site	×	×	×	√	×
Testing	√	×	×	×	×
Maintenance - Updated	√	×	√	√	×
Level of Confidence	🟢	🔴	🟡	🟡	🔴

Conclusion

Inconsistency in management of Business Continuity Plans has been identified.

Appendix C –Documents reviewed

Whilst conducting the audit we had regard to the following:

OCC Risk List Nov 2007
BIA workshop findings OCC
BRO Final Report v1
OCC Recovery Plan v11
BCP Customer Services v01
BCP Business Systems v01
BCP Revenues and Benefits v01
BCP Oxford City Homes v01
BCP Human Resources v01
BCP Environmental Health v01
BCP Customer Services v02
BCP Business Systems v01
BCP Revenues and Benefits v02
BCP Oxford City Homes v02
BCP Human Resources v021
BCP Environmental Health v03

The following staff were interviewed:

Mike Newman – Corporate Secretariat Manager
Daniel Hennessy - Business Systems Manager
Paul Warters – Revenues and Benefits Manager
Claire Osbourne – Human Resource Manager

Adrienne Linguard – Project Manager, Business Transformation
John Copely – Head of Service, Environmental Health
Paula Pearce - Application Systems Specialist

Appendix D - Summary of work undertaken and risks reviewed

Our work involved:

- identifying the processes and plans in place by reviewing documents and discussions with senior staff including Corporate Secretariat, ICT, Revenues and Benefits, Human Resources, Environmental Health and Oxford City Homes;
- Assessing the processes against Section 11 of Manual of Protective Security (MoPS);
- evaluating the adequacy of existing processes and plans; and
- highlighting areas for improvement and/or streamlining.

Work Undertaken	Risks Reviewed
We have reviewed Business Continuity Planning and associated process which are a core component of corporate risk management and emergency planning and allow for an acceptable interim level of service and the restoration of full services at a determined point in time. Our work included the following areas: • Risk Assessment; • Business Continuity Plans; • Testing; • Maintenance; and • Awareness of business continuity planning issues and training.	• Risk are not identified and mitigated against leading to major loss of a critical business process. • Inadequate response to an event leads to failure to restore critical business process • Plans are not effective or updated leading to failure to restore critical business process • Staff are not aware or trained in their business continuity planning roles leading to failure to restore critical business process

INFRASTRUCTURE, GOVERNMENT AND HEALTHCARE

Review of Information and Data Security 2008/09

Overall system rating:	
▦	🟥 Weak

Oxford City Council

7 November 2008

Report status	
Date of Debrief	5 September 2008
Discussion draft issued	30 September 2008
Management responses received	7 November 2008
Final report issued	7 November 2008
Presented to Audit and Governance Committee	25 November 2008

Distribution for action	Distribution for information
Daniel Hennessy, Business Systems Manager	Penny Gardner/Sarah Fogden, Head of Service – Finance Ben Brownlee – Head of Transformation

AUDIT ▪ TAX ▪ ADVISORY

Executive Summary

Conclusion

As internal auditors of the Authority we are required to give an annual overview of the system of internal control. In arriving at this overview, we give a conclusion on the individual systems reviewed during the year. Our conclusion is either that the system is good, satisfactory, weak or unacceptable. However, in giving our conclusion, it should be acknowledged that our work is designed to enable us to form an opinion on the quality of the systems examined, based on the work undertaken during our current review. It should not be relied upon to disclose all weaknesses that may exist and therefore the conclusion is not a guarantee that all aspects of the systems reviewed are adequate and effective.

From the work performed on information and data security, we consider there is considerable risk that the controls currently in place will fail to meet their objectives. We have identified that the Authority does not have a nominated Information Security Officer, or a formal group set up to manage and monitor information security issues on a regular basis. In addition, although there is a general ICT Security Policy, there is no detailed Information Security Policy covering wider aspects of information and data security. We also identified that the Authority does not have any data sharing protocols in place and does not have a formal policy on electronic and manual data and information retention/disposal. As a result, we have graded area as weak

We have made seven recommendations which will address the identified weaknesses. The implementation of our recommendations should enhance data security and provide an increased level of assurance to the Authority and management from the date of implementation.

Context

The audit of information and data security has been identified as part of the internal audit for 2008/09 approved by the Audit and Governance Committee. The objectives of our review, as outlined in the terms of reference were to assess the effectiveness of existing data security operating within the Authority, including data security management and awareness.

The objective of information and data security is to protect the confidentiality, integrity and availability of all Authority data/information. Following the recent high profile data losses in the Public Sector, measures have been implemented by Government to examine and improve data handling. There are a number of good practice documents which cover data and information security including the Manual of Protective Security (MoPS), ISO 27001 (the current standard for Information Security Management), Principle 7 of the Data Protection Act 1998 as well as the recent guidance issued by the Cabinet Office, Data Handling: Procedures in Government.

As part of this review, we have evaluated compliance against the core aspects of the good practice guidance. The scope of the review did not include the security of the large amounts of information and data which is held manually.

During our review we were provided with information for a number of areas including Business Services, Customer Services, Environmental Health, Oxford City Homes and Human Resources. We also reviewed supporting documentation as listed in Appendix 1.

Acknowledgement

We would like to take this opportunity to thank your staff for their assistance and co-operation during our time on site.

1. Executive summary (cont'd)

This section of the report highlights the main findings of our review. Further details, together with our recommendations, are included in the 'detailed findings and recommendations section' of the report which can be found from page 25.

Information and Data Security		
Objective	**Areas of good practice**	**Areas for further development**
To review the controls which ensure that the security, integrity and confidentiality of information and data is being maintained.	Our review identified the following areas of good practice in respect of the Authority's Information/ Data Security arrangements; ✓ The Authority has an ICT Security Policy that outlines basic information security rules and protocols for hardware, software, and electronic data. ✓ Corporate induction training includes areas of data security and confidentiality, as well as general awareness of issues relating to the Data Protection Act 1998. ✓ A programme of laptop encryption is in place with roll-out to be completed by January 2009.	Our work has also identified the following areas where controls could be further strengthened: ▪ A more detailed Information Security Policy should be prepared and approved by the Council. This revised policy should include additional information outlined in recommendation 1 of this report. ▪ The Authority should develop management arrangements for Information Security and establish an Information Security role and consider setting up a formal group that discusses information security issues on a regular basis. ▪ Data sharing should be formally controlled and staff provided with guidance on who data can be shared with, and how it should be protected. Formal data sharing protocols should be fully documented and agreed. ▪ A structured information security training programme should be provided for all appropriate computer/information users in the Council. ▪ Data Retention guidance should be produced and archived data should be reviewed to ensure it is being stored appropriately. ▪ An Incident Management process should be implemented to ensure potentially serious information security issues are reported to appropriate officers and corrective action taken. ▪ Procedures relating to the retention of backup media should be fully documented, communicated to key staff and ensure they are complied with at all times.

The table below details the number of recommendations made, the priorities assigned and those accepted by management.

	Priority One	Priority Two	Priority Three	Total
Made	2	5	0	7
Accepted	2	5	0	7

2. Detailed findings and recommendations

We have assessed each finding in our report and assigned to it a priority, as follows:

Priority rating for recommendations raised		
Priority One: Issues arising referring to important matters that are fundamental to the system of internal control. We believe that the matters observed might cause a business objective not to be met or leave a risk unmitigated and need to be addressed as a matter of urgency	*Priority Two*: Issues arising referring mainly to matters that have an important effect on controls but do not require immediate action. A business objective may still be met in full or in part or a risk adequately mitigated but the weakness represents a significant deficiency in the system.	*Priority Three*: Issues arising that would, if corrected, improve internal control in general but are not vital to the overall system of internal control.

#	Priority	Issue	Risk	Recommendation	Management Response
1	●One	**Information Security Policy** The Authority has an ICT Security Policy which includes information on controls over computer hardware, software and aspects of electronic data. A separate Information Security Policy has not been developed encompassing wider aspects of ICT security and information security issues such as data and information handling, information ownership, records management, asset management, systems development and maintenance, business continuity management, and include procedures for managing information security related incidents. As part of the review we also identified the Data Protection Policy was dated 2004 and did not reflect all elements of Data Protection as per the 1998 Act.	Policy and Procedures for Information/Data Security may be unclear.	The Authority should develop a more detailed Information Security Policy that includes further information including information and data handling, information ownership, systems maintenance and development, business continuity management and processes for dealing with information security related incidents. The revised policy should be subject to version control and reviewed annually. The Data Protection Policy should be reviewed and updated.	Agreed. We will develop a detailed Information Security Policy as part of our Information management project including an update of Data Protection Policy and Incident Management processes. Martin Hughes 30 Jan 09

2. Detailed findings and recommendations (cont'd)

#	Priority	Issue	Risk	Recommendation	Management Response
2	● One	**Management Arrangements** Although ICT security rests within Business Services, the Authority has not formally established management arrangements for overall information and data security, covering both electronic and manual data/information. The Authority has not appointed or nominated an officer as an Information Security Officer/Information Asset Owners, nor has it developed a dedicated group made up of IT and departmental staff that meets regularly to discuss information security issues, processes and procedures.	Accountability for information/ data security may not be clear.	The Authority should develop its management arrangements for Information / Data security and should consider developing the role of an Information Security Officer / Information Asset Owners and consideration should be given to the setting up of an Information Security Group made up of IT and appropriate departmental staff.	Agreed. We will develop and appoint the role of an Information Security Officer (part time) and Information Asset Owners (part time). We will also set up an Information Security Group made up of IT and appropriate departmental staff. Ben Brownlee 30 Jan 09
3	● Two	**Data Sharing** Although the Authority shares data with a number of external organisations, no data sharing protocols have been implemented. We identified that a number of insecure data transfers take place on a regular basis including: • medical records sent from the Occupational Therapy Department by either letter, telephone or unencrypted email to the Health Protection Agency; • information and data sent as an email attachment to HMO Licensing; • individual case data sent to HMRC by email with no security safeguards such as encryption or password protection; and • Revenues and Benefits Department send information without security safeguards such as encryption to the Department of Work and Pensions (DWP).	Confidential and personal information may be accessed and misused.	Formal Data Sharing Protocols should be documented and agreed. Data sharing should be formally controlled and staff provided with guidance on who data can be shared with, and how it should be protected.	Agreed. We will document Formal Data Sharing Protocols in the Services, this will be coordinated centrally with guidance to staff issued. Martin Hughes and IT areas from Services 28 Feb 09

2. Detailed findings and recommendations (cont'd)

#	Priority	Issue	Risk	Recommendation	Management Response
4	● Two	**Data Retention / Destruction** There is no corporate guidance on the secure destruction of confidential or personal data, nor is there any guidance on data retention. As part of the review we identified that confidential waste is being insecurely stored in sacks prior to disposal. We also identified that in some departments, information and data was being kept indefinitely, which results in a potential breach of the Data Protection Act 1998.	Confidential information may be accessed and misused.	A formal Data Retention and Destruction Policy should be produced and approved. Appropriate secure storage facilities should be provided for confidential waste. Any data that is archived should be reviewed periodically to ensure it is being stored appropriately and securely.	Agreed We will produce a formal Data Retention and Destruction Policy as part of the Information Management Project. Martin Hughes 28 Feb 09 We will investigate secure storage options and recommend a solution (likely to be one secure bin for confidential waste by floor). Bob Taylor 30 Nov 08
5	● Two	**Staff Awareness / Training** Several of the staff members interviewed were unclear of the distinction between subject access requests under the Data Protection Act 1998 and the Freedom of Information Act 2000. We identified that specific training on information security related issues is not given apart from some high level information provided to staff as part of the corporate induction program. We understand that some departments provide email reminders and updates.	Inappropriate procedures may be adopted.	Improved information security training and awareness should be carried out by the Authority. This could be delivered by a structured information security training programme with levels of training provided in accordance with the roles and responsibilities of computer / information users.	Agreed. We will produce an induction training slide for new staff and we will produce and hold training for specific staff groups, with HR. Martin Hughes and Andy Davice 31 Mar 09

2. Detailed findings and recommendations (cont’d)

#	Priority	Issue	Risk	Recommendation	Management Response
6	●Two	**Information Security Incident Handling** No guidance or procedures exist for information security related incident reporting or handling. Without these, there is the risk that information security issues/breaches of information security may not be given the required level of priority and potentially serious information security issues may not be reported to an appropriate officer with corrective action taken.	Inconsistent practices may occur.	An Incident Management process should be implemented to ensure all information security related incidents are reported, investigated and addressed in a consistent manner.	Agreed. We will produce an incident management process alongside the Information and Data Security policy. Martin Hughes 23 Dec 08
7	●Two	**Backups** Our discussions with senior IT staff identified there is no formal backup policy which has resulted in a lack of clarity over how long back up media is retained before being overwritten.	Critical information may not be available when it is required.	Senior IT staff should ensure that all procedures relating to the retention of backup media are fully documented and communicated to key staff.	Agreed. We will produce a formal backup policy and communicate this to staff. Martin Hughes 31 Mar 09

Appendix 1 –Documents Reviewed/Officers Interviewed

Whilst conducting our work, we reviewed the following policies and documents, and met with the officers as detailed:

General:

- IT Security Policy;
- Statement of Freedom of Information policy (from Council website);
- Freedom of Information training pack (Council intranet);
- Data Protection Policy dated Jan 2004;
- Data Protection Act 1998 roles/responsibilities;
- Authority for Disclosure forms.

Human Resources Department:

- Employee Handbook (currently under review);
- New Starter Checklist (covering confidentiality briefing);
- Draft Employee Code of Conduct;
- Employment Application form.

Revenues and Benefits Department:

- Confidentiality Agreement form (concerning DWP information);
- Sample training timetable for employee (covering confidentiality/data protection);
- Document Retention Policy.

Officers Interviewed:

- Daniel Hennessy, Business Systems Manager
- Ellen Devanney, HR Service Officer
- Paul Wilding, Council Tax Manager
- Roy Summers, Finance Manager
- Anne Harvey-Lynch, Revenues Manager
- Vicki Fensome, Information Systems Manager
- Martin Hughes, ICT Project Manager and Interim FOI Officer
- Sean Fry, Operations Support Manager
- Sue Cudden, Fleet Manager
- Tony Payne, Environmental Development
- Gail Siddall, HMO Licensing and Health & Safety
- Phil Adlard, Revenues and Benefits
- Martyn Mumford, Oxford City Homes

Appendix 2 - Data Handling Procedures in Government

We have documented below what government departments are currently in the process of doing to adopt best practice in information risk management. The Authority should review its processes in light of the details below.

- Defining an information risk policy, which says how

– information will be managed within the organisation and their delivery partners and how effectiveness will be assessed;

– identifying information assets, and senior individuals involved in running relevant operations as named Information Asset Owners which have clear responsibility for information and date;

– assessing risks to the confidentiality, integrity and availability of information, and putting in place responses to manage those risks as necessary;

– specifying an annual process of assessment to provide an evidence base to support the effectiveness of processes adopted;

- Formalising the role of Senior Information Responsible Officer to oversee the process;
- Identifying what personal data is held and used that falls into the new definition of "protected personal data";
- Establishing procedures and policies to ensure such data is handled as if they are protectively marked;
- Developing an encryption programme for such data, where it is on removable media, except where that is not possible, for example because of the need to access back-ups;
- Where such data is stored electronically, minimising the use of removable media and the amount of data transferred to them, and minimise the user rights to copy files onto such media;
- Introducing arrangements for secure disposal of paper and electronic records;
- Reviewing procedures for reporting information risk incidents;
- Amending HR policies and guidance as necessary;
- Publishing Information Charters; and
- Compiling material on breaches.

Appendix 3 – Summary of work undertaken and risks reviewed

Our work involved:

- identifying and documenting controls in place by discussions with staff across the Authority;
- testing key underlying controls to confirm they are operating effectively where appropriate;
- evaluating the adequacy of existing processes and controls; and
- highlighting areas for improvement and/or streamlining.

Area	Summary of work undertaken	Summary of risks reviewed
Information/ Data Security	We have reviewed the processes in place which ensure the security of information and data. We have assesses the Authority against key areas as detailed within best practice as documented in the following: • Manual of Protective Security (MoPS); • ISO 27001 (the current standard for Information Security Management); • Principle 7 of the Data Protection Act 1998; • Data Handling; Procedures in Government. .	• The security of IT systems is compromised and/or data is lost, damaged, unavailable or unlawfully disclosed to unauthorised persons. • Agreed security standards have not been implemented, leading to the security of data/information systems being compromised and/or data being lost or unavailable.

Performance Information

Performance indicators

We have documented below the performance against the indicators included in the Protocol for the routine internal audit reviews:

Performance Area	**Performance Target**	**2008/09** **Performance to date**
Issue Terms of Reference	15 days before start on site (target 100%)	100% (10 out of 10) ☺
Issue Draft Report	Within 15 days of final debrief (target 100%)	100% (4 out of 4) ☺
Management response to routine audit reports	Within 15 days of draft report (target 100%)	25% (1 out of 4) ☹
Issue Final Report	Within 10 days of management responses (target 100%)	100% (4 out of 4) ☺

We have documented prior year performance below for information:

Performance Area	Performance Target	2007/08 Performance	2006/07 Performance	2005/06 Performance
Issue Terms of Reference	15 days before start on site (target 100%)	88.9% ☺	88.9% ☺	66.6% ☹
Issue Draft Report	Within 15 days of final debrief (target 100%)	64.7 % ☹	83.3% ☺	83.8% ☺
Management response to routine audit reports	Within 10 days of draft report (target 100%)	23.53% ☹	55.5% ☹	50% ☹
Issue Final Report	Within 10 days of management responses (target 100%)	100% ☺	100% ☺	100% ☺

Audit and Governance Committee reporting schedule

Audit and Governance Committee Date	Proposed reports	
25th June 2008	•Progress report 1	
24th July 2008	•Progress update	
23th September 2008	•Progress report 2	•Taxi Licensing •Car Parking
25th November 2008	•Progress report 3	•Business Continuity/Disaster Recovery •Data Security
27th January 2009	•Progress report 4 •Housing Repairs •Local Financial Systems •Payroll •Treasury Management	•Benefits •Local Taxation •Housing Repairs •Fixed Assets
24th March 2009	•Progress report 5 •Core Financial Systems (AR/AP/MAS) •Building Control/Planning/Enforcement	•Single Status Model •Corporate Governance •Leaseholders •Health and Safety Follow up
28th April 2009	•Annual report	