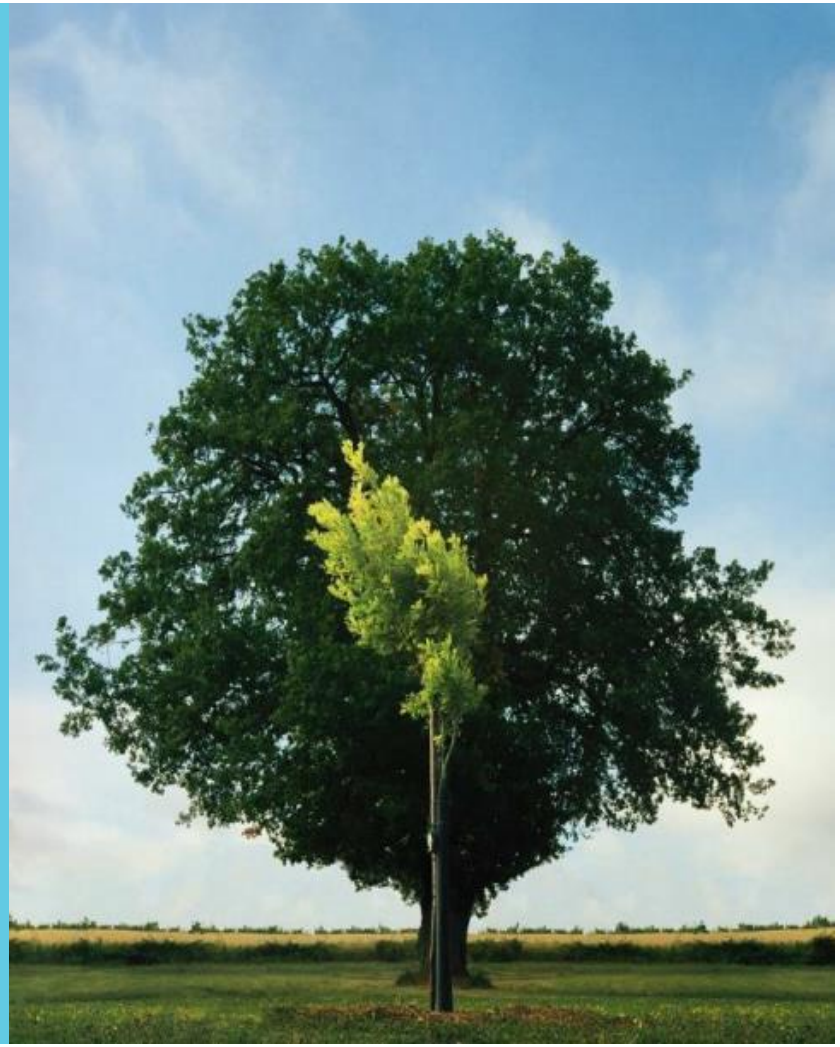
Oxford City Council

INTERNAL AUDIT REPORT

Audit 6. Business Continuity and Disaster Recovery

November 2016

LEVEL OF ASSURANCE	
Design	Operational Effectiveness
Limited	Limited



BDO

Agenda Item 5

CONTENTS

36

REPORT STATUS	
Auditors:	David Harvey, Assistant Manager
Dates work performed:	5 September – 27 October
Draft report issued:	Initial: 17 November 2016 Revised: 8 February 2017
Final report issued:	**16 February 2017**

DISTRIBUTION LIST	
Jacqueline Yates	Executive Director – Organisational Development and Corporate Services
Nigel Kennedy	Section 151 Officer
Helen Bishop	Head of Business Development
Vic Frewin	Chief Technology Officer

EXECUTIVE SUMMARY

CLIENT STRATEGIC RISKS	
Risk	Efficient, effective Council

LEVEL OF ASSURANCE (SEE APPENDIX II FOR DEFINITIONS)		
Design	Limited	System of internal controls is weakened with system objectives at risk of not being achieved.
Effectiveness	Limited	Non-compliance with key procedures and controls places the system objectives at risk.

SUMMARY OF RECOMMENDATIONS (SEE APPENDIX II FOR DEFINITIONS)	
High	4
Medium	3
Low	

Total number of recommendations: 7

OVERVIEW

The purpose of our review was to provide assurance that appropriate arrangements are in place and operating effectively in relation to business continuity and disaster recovery. As a Category One organisation, as defined by the Civil Contingencies Act 2004, the Council has a statutory obligation to establish and maintain effective business continuity management arrangements. Responsibility for the implementation and management of the Council's continuity planning has been assigned to Financial Services, having previously been managed by the Corporate Affairs Lead within Law and Governance. Our review included an assessment of the Council's business continuity plans including those in place for its Contact Centre and Leisure Centres. The Council's leisure centres are managed by a third party, Fusion.

Areas of good practice identified were:

- The Council has established a standard format for its business continuity plans, which can be easily replicated
- The Council has a defined procedure in place for the invocation of its Corporate Business Continuity plan.

However, we have identified the following seven areas for improvement:

- The Council's services have not been assessed in order to determine their criticality to the Council (High – Finding 1)
- The business continuity plans for the Council's services were found to be incomplete, inaccurate or missing (High – Finding 2)
- There is not an effective process to manage the Council's continuity planning to provide central oversight (High – Finding 3)
- There is not a defined IT Disaster Recovery plan in place (High – Finding 4)
- The Council's business continuity and disaster recovery plans are not tested on a routine basis (Medium – Finding 5)
- The viability of the Council's alternative recovery site at Horspath Road has not been assessed (Medium – Finding 6)
- Members of staff with responsibility for continuity planning are not provided with adequate training. (Medium – Finding 7)

The Council's ability to provide its critical services in the event of an incident is undermined by the absence of effective business continuity management arrangements. Business continuity plans for the Council's services were found to be missing and, where they have been defined, the business continuity plans were found to be incomplete or contain information that is out of date. Consequently, we conclude limited assurance over both the design and effectiveness in relation to the Council's business continuity and disaster recovery management arrangements.

DETAILED RECOMMENDATIONS

RISK: The Council may not fully assess key threats or risks to the continuity of business and IT operations			
Ref.	**Finding**	**Sig.**	**Recommendation**
1	It was observed during our fieldwork that the Council has not completed either a risk assessment or business impact assessment in order to determine the criticality of its services and to prioritise their recovery. Annex 2 of the Council's Corporate Business Continuity Plan (the Plan) includes a record of the Council's services organised by criticality. However, the Plan does not establish the rationale for prioritising the recovery of the Council's services or accurately define the maximum possible time that the Council could function without each service. Our review of the continuity plans that are in place for the Council's services found that the recovery arrangements in place are not aligned to the Plan with regards to prioritisation of the recovery of individual services. Furthermore, the Plan has not been reviewed since January 2014 and refers to a Corporate structure that has been significantly changed. This is highlighted by the fact that ICT has not been included within the Council's list of critical services. Not determining the criticality of the Council's services and prioritising their recovery accordingly increases the risk of the Council being unable to provide its critical services, including those that it is statutorily required to provide, due to insufficient continuity arrangements.	High	Senior management must require that all Council services complete a risk assessment and a business impact assessment in order to determine and define their Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) according to: • Financial impact on the Council of the loss of a service • Reputational impact on the Council of the loss of a service • Regulatory impact on the Council of the loss of a service • Resources required to recover the service. The outcome of this review should be used to define the priority for the recovery of the Council's services according to: • Their criticality to the Council and its strategic objectives • The maximum possible time that the Council can operate without providing the service. All business continuity plans should be reviewed and, where necessary, updated so that they reflect the corporate prioritisation and that resources are adequately allocated to recover the Council's critical services. Furthermore, senior management should review the criticality of its services on an annual basis or following a significant change to its structure.

DETAILED RECOMMENDATIONS

RISK:	
MANAGEMENT RESPONSE	**RESPONSIBILITY AND IMPLEMENTATION DATE**
The areas where there are missing or out of date Business Continuity Plans are being identified to the Heads of Service Group and the respective Heads of Service will be tasked to produce or update plans for their areas. The Council's insurers and Risk Management advisors, Zurich, have been engaged to facilitate the Council in improving and updating the Council's Business Continuity arrangements. The review of the overall arrangements has been incorporated into this piece of work. The Heads of Service Group will be tasked to prioritise the criticality of all Council services.	***Responsible Officer:*** Nigel Kennedy, Head of Financial Services ***Implementation Date: End April 2017***

DETAILED RECOMMENDATIONS

RISK: Business Continuity Plans are inadequate leading to a delay in or failure to recover systems, preventing adequate delivery of services in a Business Continuity incident			
Ref.	**Finding**	**Sig.**	**Recommendation**
2	It was observed during our fieldwork that there are a number of Council services that do not have business continuity plans that are complete, accurate or are aligned to the Council's Corporate Business Continuity Plan. The following three services were found not to have continuity plans in place: • The services overseen by the office of the Assistant Chief Executive • Leys, Rose Hill, and Barton Regeneration Teams • Sustainability Team • Welfare Reform Team. Additionally, the following services were found to be included as part of legacy continuity plans that are not reflective of the Council's corporate structure: • Planning and Regulatory that, in the event of an incident, would rely on the City Development and Environmental Development plans that were last reviewed in January 2015 and November 2014 respectively • Council Tax, Housing Benefits Administration, Housing Rents, Business Rates and Procurement that, in the event of an incident, would rely on the legacy Customer Services continuity plan are now the responsibility of Financial Services. Our review indicated that the Council's business continuity plans do not include: • How the IT hardware necessary to continue to provide critical services is to be provided or acquired • The Recovery Time Objective (RTO) for critical IT services for each Council service • Complete and up to date contact lists, which includes the contact information for third party suppliers.	High	Senior Management must undertake a review of the Council's business continuity plans, including its Corporate Business Continuity plan, and, where necessary: • Revise existing plans so that they are aligned to the Council's corporate structure • Business continuity plans are defined for the Council's services that are found not to have existing plans. Senior management must require all continuity plans include a record of all information necessary to continue the Council's services in the event of an incident, including but not limited to: • The provision or acquisition of IT hardware • The Recovery Time Objective for critical IT services • Complete and up to date contact lists. Senior management should consider the establishment of a Business Continuity Policy that defines the Council's requirements for continuity planning. Furthermore, senior management must make appropriate arrangements for accessing business continuity plans in the event of an incident.

DETAILED RECOMMENDATIONS

RISK: Business Continuity Plans are inadequate leading to a delay in or failure to recover systems, preventing adequate delivery of services in a Business Continuity incident (Cont.)			
Ref.	**Finding**	**Sig.**	**Recommendation**
2	Of the business continuity plans reviewed, we found that: • Four plans had been reviewed in the last year • Six plans had not been reviewed since 2014 • The plan provided by Fusion for the recovery of the Council's Leisure Centres had not been reviewed since 2011. Furthermore, the Council does not have adequate arrangements in place to access its continuity plans in the event of an incident. Incomplete, inaccurate or plans that are not aligned to the Council's corporate structure increase the risk that the Council is unable to provide its critical services in the event of an incident.	High	
MANAGEMENT RESPONSE			**RESPONSIBILITY AND IMPLEMENTATION DATE**
The Council's insurers and Risk Management advisors, Zurich, have been engaged to facilitate the Council in improving and updating the Council's Business Continuity arrangements. This includes a review of a the Council's business continuity plans, including its Corporate Business Continuity plan. The establishment of a Business Continuity Policy will be considered and discussed with Zurich. The Heads of Service Group will be tasked with ensuring that there are appropriate arrangements for accessing business continuity plans in the event of an incident.			***Responsible Officer:*** Nigel Kennedy, Head of Financial Services ***Implementation Date: End March 2017***

DETAILED RECOMMENDATIONS

RISK: Plans are not reviewed, kept up to date or tested			
Ref.	**Finding**	**Sig.**	**Recommendation**
3	The responsibility for producing Business Continuity Plans rests with each Head of Service. The Head of Financial Services has responsibility for co-ordinating the plans and operationally this is delivered by the Financial Accounting Team led by the Financial Accounting Manager. During our testing it was identified that the Council does not have a procedure in place to determine: • Status of each plan, including missing or incomplete information • Last recorded review date for each plan • Last recorded test date for each plan • Status of third party plans. The absence of an appropriate business continuity management system increases the risk of the Council's continuity arrangements becoming unfit for purpose.	High	Management should establish a business continuity management system that provides oversight of the status of the Council's business continuity and disaster recovery arrangements, including but not limited to: • Last recorded review date for each plan • Last recorded test date for each plan • Status of each plan, including where plans are incomplete • Status of third party plans.
MANAGEMENT RESPONSE			**RESPONSIBILITY AND IMPLEMENTATION DATE**
Agreed.			***Responsible Officer:*** Nigel Kennedy, Head of Finance ***Implementation Date: March 2017***

DETAILED RECOMMENDATIONS

RISK: Planned dependency on IT functionality is not sufficiently co-ordinated between Business Continuity and Disaster Recovery activities			
Ref.	**Finding**	**Sig.**	**Recommendation**
4	The Council has outsourced responsibility for the management of its IT infrastructure to a third party, SCC. SCC are responsible for the recovery of the Council's IT infrastructure, however validation of these arrangements has not been verified by the Council although the Council have begun greater engagement with SCC over their arrangements and testing plans. It was observed during our fieldwork that the Council does not have a finalised, tested and approved IT Disaster Recovery Plan in place. Whilst the Council has a scenario based plan in place for responding to an incident within IT, it would not be sufficient to recover the Council's critical IT infrastructure and systems as it does not include detailed, technical or recovery information. Furthermore, our review of the Council's business continuity plan indicated that there is a lack of awareness as to the recovery time and point objectives for critical IT systems. As part of the review Internal Audit, the Council and SCC held a teleconference in December 2016 to discuss appropriate controls to improve arrangements in place. Since then the Council have set out a position statement on current progress and have plans to implement recommendations raised. The absence of a defined IT Disaster Recovery plan increases the risk of the Council being unable to recover its critical IT infrastructure, hardware and systems in the event of a disaster.	High	Senior Management must produce a defined IT Disaster Recovery Plan that is aligned to the Council's continuity arrangements and includes, but is not limited to: • The recovery time and recovery point objectives for IT infrastructure and systems • The procedures for invoking the Plan in the event of a disaster • The procedures and information necessary for communicating with all key members of staff within IT and the wider Council • The procedures for recovering the Council's critical IT infrastructure and systems • The contact information for all third party IT suppliers. Furthermore, Senior Management should require that all third parties involved in the recovery of the Council's IT arrangements provide assurance that their disaster recovery plans are adequate.
MANAGEMENT RESPONSE			**RESPONSIBILITY AND IMPLEMENTATION DATE**
SCC has provided written assurance that they have mature end to end building, infrastructure and Service Continuity plans in place, which underpin their Sentinel services offering. Furthermore SCC have provided certifications which give independent assurance over the build and PSN compliance of the platform they have in place. Discussions and greater engagement has commenced and this has resulted in an outline agreement to test each of applications the Council have (there are over 100) in 4 bundles split into each quarter - the first test is expected to commence in March 2017. Every 5th quarter, the entire dual-site environment will be tested by a full production failover. *We accept the findings identified and have made progress since the audit to devise long term solutions to ensure regular and robust testing of our platforms supported by Council approved plans are in place.*			***Responsible Officer:*** Helen Bishop, Head of Business Improvement ***Implementation Date: March 2017 (first test commenced).***

DETAILED RECOMMENDATIONS

RISK: Plans are not reviewed, kept up to date or tested			
Ref.	**Finding**	**Sig.**	**Recommendation**
5	It was observed during testing that the Council does not have a requirement for its business continuity and disaster recovery plans to be fully tested on a routine basis. The last recorded test of the Council's business continuity plans was a table top, scenario based exercise performed in May 2015. The Council's IT Disaster Recovery arrangements have not been subject to a full test. Not testing the Council's business continuity and disaster recovery plans increases the risk that the Council is unable to recover its critical services in the event of an incident as a result of a previously unidentified issue or gap.	Med	Management should require that the Council's business continuity and disaster recovery plans are tested on at least an annual basis or following a significant change. The results of all testing performed should be reported to senior management for review.
MANAGEMENT RESPONSE			**RESPONSIBILITY AND IMPLEMENTATION DATE**
The Council's Business Continuity Plans were last tested in 2015. The Council's insurers and Risk Management advisors, Zurich, have been engaged to facilitate the Council in improving and updating the Council's Business Continuity arrangements. This includes a test of updated Corporate and service business continuity plans which will be undertaken during 2017.			***Responsible Officer:*** Bill Lewis, Financial Accounting Manager ***Implementation Date: December 2017***

DETAILED RECOMMENDATIONS

RISK: Operational and IT recovery options may not be defined and arrangements may not be in place for standby business and IT facilities in the event of a major failure or disaster			
Ref.	**Finding**	**Sig.**	**Recommendation**
6	The Council has identified its offices on the Horspath Road as being the alternative recovery site for its services. Through our review of the Council's business continuity plans it was identified that up to 52 people would need to be able to access these offices in the event of an incident on the first day. It should be noted that for the Customer Contact Centre the Council regularly (monthly) undertake reviews over the adequacy of capacity at Horspath Road to accommodate the Contact Centre. There are twelve computer terminals allocated to support a business continuity incident for the Contact Centre and tests to verify these are fit-for-purpose occur monthly. Whilst saying the above the Council's business continuity plans do not with regards to Horspath Road outside of the Customer Contact Centre do not include: • Arrangements for relocating members of staff to the Horspath Road offices or the time it would take • Arrangements that are in place to provide sufficient resources to allow members of staff to continue to work • Whether there is sufficient capacity at the site to accommodate the number of people recorded within the Council's continuity plans. Not adequately preparing for the relocation of staff to an alternative recovery site increases the risk of the Council being unable to continue to provide its critical services in the event of an incident.	Med	Management should review the use of its Horspath Road offices to support the continuity of its critical services. Where necessary, management should consider identifying alternative locations or the use of remote working facilities. Business continuity plans should be updated to include how members of staff would get to and from its alternative locations in the event of an incident.
MANAGEMENT RESPONSE			**RESPONSIBILITY AND IMPLEMENTATION DATE**
The Council's insurers and Risk Management advisors, Zurich, have been engaged to facilitate the Council in improving and updating the Council's Business Continuity arrangements. This includes a review of the use of Horspath Depot and ensuring that procedures around access to the Depot (or alternative site(s)) are included in plans.			***Responsible Officer:*** Bill Lewis, Financial Accounting Manager ***Implementation Date: December 2017***

DETAILED RECOMMENDATIONS

RISK: The Council may not have an appropriate business continuity management framework in place			
Ref.	**Finding**	**Sig.**	**Recommendation**
7	It was observed during our fieldwork that the Council does not have a defined procedure in place for providing business continuity management training to all members of staff that are involved in the Council's continuity planning. Not providing members of staff with appropriate business continuity management training increases the risk that the Council is unable to continue to provide its critical services in the event of an incident as members of staff are unaware of the correct action to take.	Med	Management should develop and deliver a training programme for business continuity management based upon the needs of members of staff that are involved in continuity and recovery planning. Furthermore, management should establish a process to raise awareness of its continuity arrangements.

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
The Council's insurers and Risk Management advisors, Zurich, have been engaged to facilitate the Council in improving and updating the Council's Business Continuity arrangements. This includes the development and delivery of a training programme in 2017.	***Responsible Officer:*** Bill Lewis, Financial Accounting Manager ***Implementation Date: End July 2017***

APPENDIX I - STAFF INTERVIEWED

BDO LLP appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and cooperation.

NAME	JOB TITLE
Bill Lewis	Financial Accounting Manager
Michael Newman	Corporate Affairs Lead
Anna Winship	Management Accounting Manager

NAME	JOB TITLE
Michelle Iddon	Customer Services Manager
Lucy Cherry	Leisure and Performance Manager
Paul Collins	ICT Operations Manager

APPENDIX II - DEFINITIONS

LEVEL OF ASSURANCE	DESIGN of internal control framework		OPERATIONAL EFFECTIVENESS of internal controls	
	Findings from review	Design Opinion	Findings from review	Effectiveness Opinion
Substantial	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non compliance with some controls, that may put some of the system objectives at risk.
Limited	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non compliance and/or compliance with inadequate controls.

Recommendation Significance	
High	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

APPENDIX III – TERMS OF REFERENCE

BACKGROUND

The Council performs a number of essential and statutory functions. Effective Business Continuity and Disaster Recovery arrangements enable the Council to restore service delivery without undue delay in the event that an unplanned event prevents normal systems and processes occurring. Good planning will enable prioritisation of work to restore affected services, and identify the key contacts, resources and processes to return to stability of operations.

Recent incidents affecting Local Authorities have highlighted the reality of the risks and the necessity for Councils to be prepared - South Oxfordshire District Council was the victim of an arson attack in 2015, and more recently Lincolnshire County Council Services were affected by a ransomware computer virus.

The inability to maintain key services in exceptional circumstances (business continuity) has been identified as a key corporate risk (no. 11). To enhance resilience, the Council has worked to an agreement with Chelmsford City Council (since 2005) for the provision of Emergency Planning functions, including Business Continuity and Disaster Recovery, and partly funds an Emergency Planning Officer employed by Chelmsford City Council. The arrangements enable shared resources and expertise, and cross Council incident support through an increased pool of trained staff.

In 2016 the responsibility for Business Continuity moved to Financial Services. A new approach to Business Continuity is expected to be taken under this responsibility and initial conversations about how to take this forward have begun.

PURPOSE OF REVIEW

The purpose of this review is to consider the design and effectiveness of the controls in place around Business Continuity and Disaster Recovery and to highlight any areas where the controls might be improved.

SCOPE OF REVIEW

The scope will cover the Key Risks set out overleaf.

EXCLUSIONS

Our work will not assess the adequacy of individual response plans, or cover the Council's legal duties under the Civil Contingency Act.

APPROACH

Our approach will be to conduct interviews to establish the controls in operation for each of our areas of audit work. We will then seek documentary evidence that these controls are designed as described. We will evaluate these controls to identify whether they adequately address the risks. Any opportunities identified to improve arrangements will be offered for consideration alongside recommendations to resolve any weakness in controls.

APPENDIX III – TERMS OF REFERENCE

KEY RISKS

Based upon the risk assessment undertaken during the development of the internal audit operational plan, through discussions with management, and our collective audit knowledge and understanding, the key risks associated with the area under review are:

- The Council may not have an appropriate business continuity management framework in place. The Council has not identified key aspects of the organisation and the critical systems, activities and resources on which they depend
- The Council may not fully assess key threats or risks to the continuity of business and IT operations.
- Business Continuity Plans are inadequate leading to a delay in or failure to recover systems, preventing adequate delivery of services in a Business Continuity event
- Plans are not reviewed, kept up to date or tested
- Business Continuity and Disaster Recovery planning processes are unnecessarily complex deterring engagement, impeding awareness or causing confusion
- Operational and IT recovery options may not be defined and arrangements may not be in place for standby business and IT facilities in the event of major failure or disaster
- Appropriate liaison may not be maintained with external parties (i.e. insurers, emergency services, suppliers, etc.)
- Planned dependency on IT functionality is not sufficiently coordinated between Business Continuity and Disaster Recovery activities.

50

DOCUMENTATION REQUEST

Please provide the following documents in advance of our review (where possible):

- A copy of the Corporate Continuity Plan
- A copy of other Corporate-wide Plans i.e. Severe Weather Plan and City Council Emergency Plan
- A copy of all the latest service area business plans
- Evidence of the desktop exercise undertaken in 2015 which assessed scenarios in service area business plans.

Any documents provided will assist the timely completion of our fieldwork, however we may need to request further documentation and evidence as we progress through the review process.

APPENDIX III - TERMS OF REFERENCE

TIMETABLE

Audit Stage	Date
Commence fieldwork	5 September 2016
Number of audit days planned	12
Planned date for closing meeting	16 September 2016
Planned date for issue of the draft report	30 September 2016
Planned date for receipt of management responses	14 October 2016
Planned date for issue of proposed final report	17 October 2016
Planned date for Section 151 and Executive Director review	14 and 21 November 2016 respectively
Papers deadline	5 December 2016
Planned Audit Committee date for presentation of report	14 December 2016

KEY CONTACTS

BDO LLP	Role	Telephone and/or email
Greg Rubins	Head of Internal Audit	t: 07583 114 121| e: greg.rubins@bdo.co.uk
Gurpreet Dulay	Internal Audit Manager	t: 07870 555 214| e: gurpreet.dulay@bdo.co.uk
David Harvey	IT Audit Assistant Manager	e: david.harvey@bdo.co.uk
Oxford City Council		
Jackie Yates	Executive Director for Organisational Development and Communications	e: jyates@oxford.gov.uk
Nigel Kennedy	Section 151 Officer	e: nkennedy@oxford.gov.uk
Helen Bishop	Head of Business Development	e: hbishop@oxford.gov.uk
Paul Fleming	Chief Technology Manager	e: pfleming@oxford.gov.uk
Mike Newman	Corporate Secretariat Manager	e: mnewman@oxford.gov.uk

SIGN OFF

On behalf of BDO LLP:		On behalf of Oxford City Council:	
Signature:		Signature:	Jackie Yates
Title:	HEAD OF INTERNAL AUDIT	Title:	Executive Director for Organisational Development and Communications
Date:	27 June 2016	Date:	28 June 2016

www.bdo.co.uk